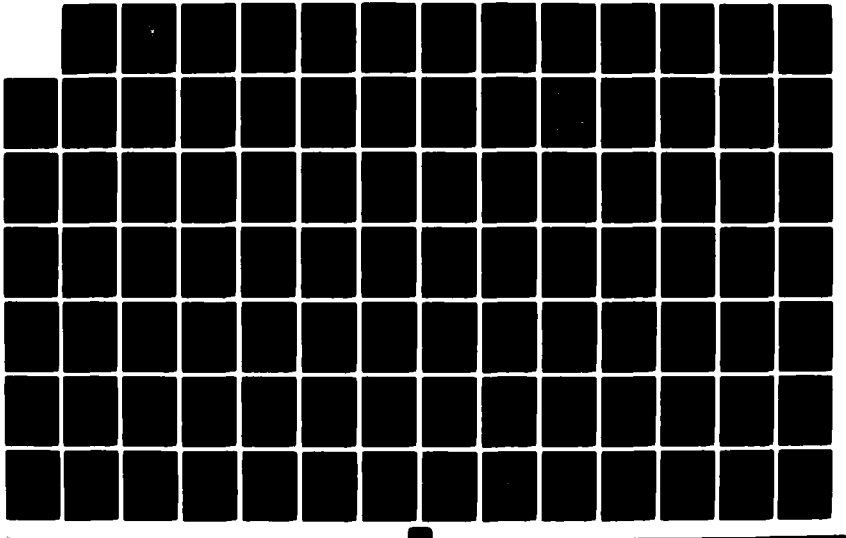
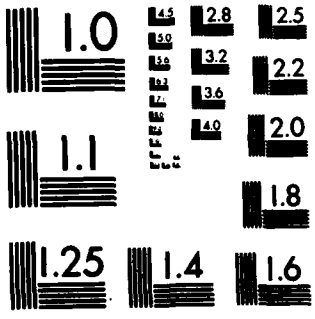
AD-A136 783 A PLAN FOR THE ACCESS AND UTILIZATION OF THE DEFENSE 1/2
DATA NETWORK BY THE UNITED STATES COAST GUARD(U) NAVAL
POSTGRADUATE SCHOOL MONTEREY CA E A LANE SEP 83

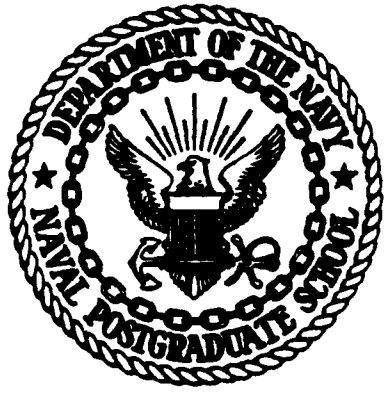
UNCLASSIFIED F/G 17/2 NL





(2)

NAVAL POSTGRADUATE SCHOOL
Monterey, California



THESIS

A Plan for the Access and Utilization of the Defense Data Network by the United States Coast Guard

By

Edward A. Lane

September, 1983

Thesis Advisor: N.F. Schneidewind

Approved for Public Release, Distribution Unlimited

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE

READ INSTRUCTIONS BEFORE COMPLETING FORM

1. REPORT NUMBER
2. GOVT ACCESSION NO.
3. RECIPIENT'S CATALOG NUMBER

4. TITLE (and Subtitle)
A Plan for the Access and Utilization of the Defense Data Network by the United States Coast Guard

5. TYPE OF REPORT & PERIOD COVERED
Master's Thesis
September, 1983

6. PERFORMING ORG. REPORT NUMBER

7. AUTHOR(s)
Edward A. Lane

8. CONTRACT OR GRANT NUMBER(s)

9. PERFORMING ORGANIZATION NAME AND ADDRESS
Naval Postgraduate School
Monterey, California 93943

10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS

11. CONTROLLING OFFICE NAME AND ADDRESS
Naval Postgraduate School
Monterey, California 93943

12. REPORT DATE
September, 1983

13. NUMBER OF PAGES
107

14. MONITORING AGENCY NAME & ADDRESS(if different from Controlling Office)

15. SECURITY CLASS. (of this report)
UNCLASSIFIED

15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)
Approved for Public Release, distribution unlimited

Accession For
NTIS GRA&I ☑
DTIC TAB ☐
Unannounced ☐
Justification
By
Distribution/
Availability Codes
Dist | Avail and/or Special
A-1

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

DTIC COPY INSPECTED

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)
Coast Guard computer networks, packet switching, Defense Data Network, local area networks, networking functional requirements

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)
This thesis presents a proposal for the integration of United States Coast Guard computer networks with the Defense Data Network. The hardware and software functional requirements for the merger are based upon a thorough understanding of packet switching and the layering of communications protocols. Results indicate that it is possible to form a hierarchical networking architecture by joining Coast Guard local-area and regional networks with the long-haul services of the Defense Data Network. Thus, computer users at each Coast Guard command level will be able to

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE
S/N 0102-LF-014-6601

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

Block 20 (Cont.)

invoke a variety of applications ranging from the handling of traditional military message traffic to the processing of sophisticated software packages.

Approved for public release, distribution unlimited

A Plan for the Access and Utilization of the Defense Data Network by the United States Coast Guard

by

Edward A. Lane
Lieutenant, United States Coast Guard
B.S., United States Coast Guard Academy, 1976

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN TELECOMMUNICATIONS
SYSTEMS MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September, 1983

Author: Edward A. Lane

Approved by: Norman F. Schneidewind
Thesis Advisor

Second Reader

Chairman, Department of Administrative Sciences

K. T. Marshall
Dean of Information and Policy Sciences

ABSTRACT

This thesis presents a proposal for the integration of United States Coast Guard computer networks with the Defense Data Network. The hardware and software functional requirements for the merger are based upon a thorough understanding of packet switching and the layering of communications protocols. Results indicate that it is possible to form a hierarchical networking architecture by joining Coast Guard local-area and regional networks with the long-haul services of the Defense Data Network. Thus, computer users at each Coast Guard command level will be able to invoke a variety of applications ranging from the handling of traditional military message traffic to the processing of sophisticated software packages.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

I. INTRODUCTION

A. BACKGROUND

The Defense Data Network (DDN) represents an attempt to apply state-of-the-art technology to provide an effective long-haul computer network. This effort has at its foundation a concept developed in the early seventies called packet switching. The U.S. Defense Advanced Research Projects Agency (DARPA) is credited with performing much of the initial research and development that will make DDN possible. DARPA was successfully able to demonstrate the credibility of packet switching as a means of computer telecommunications through a network that would eventually be known as the ARPANET [Ref.1: p.4]. The ARPANET transcended its initial experimental nature to become a viable, operational means of exchanging communications between heterogeneous computer systems. For the first time, it became convenient and economical for computers with different operating systems, made by different manufacturers, to share resources on a large scale basis.

The results of a research project do not directly lead to the same findings in a non-controlled environment. The ARPANET is continuously undergoing revision. Many of the theoretical ideas that dealt with the network were found to be inadequate when put into practice and have consequently

been modified or replaced. The Department of Defense (DOD) has determined however, that an approach similar to the ARPANET can be used to meet the computer networking needs of the armed forces. Consequently, the contract for the second generation of the Automated Digital Network (AUTODIN II) was terminated in favor of further development of ARPANET concepts to form DDN [Ref. 2: p. 1]. The results of these decisions will not be known until 1986 when DDN becomes fully operational.

B. THE PROBLEM

The United States Coast Guard is a subscriber to the AUTODIN system (AUTODIN I). The Chief of U.S. Naval Operations has requested that the Coast Guard define its computer networking requirements so that the Coast Guard may become a subscriber to the replacement Defense Data Network. DDN will provide data communication services that extend beyond the handling of traditional military message traffic to the processing of all forms of computer data. This means that the Coast Guard has the opportunity to take advantage of these new services to vastly improve the capability of its own network architecture.

The Coast Guard has also pursued the integration of multiple types of information through common networks. This effort has proceeded independently of Defense Data Network development. The major theme of this thesis is to resolve

those issues surrounding the incorporation of DDN into the Coast Guard's overall networking structure. It is theoretically possible for the Coast Guard to meet all of its data communications needs through the integration of networks developed by the service and the Defense Data Network. The overriding concern is that Coast Guard data exchanges take place in the most effective and efficient manner possible. This implies that network boundaries be appropriately defined and the transmission of data between networks be achieved in a timely and error free fashion. The result is a comprehensive, hierarchical network architecture that allows all Coast Guard users to process computer applications. It should be noted that this thesis deals with applying the latest theoretical networking advances to make the architecture possible. There is no intention to profess that the findings herein will directly lead to an operational solution to all networking difficulties. This is particularly true in the area of software development for multiple network compatibility. However, this thesis may serve as an excellent starting point for additional research, testing, and evaluation. The fact that the Coast Guard is a relatively small service, with a dedication to implementing the most recent computer technological discoveries, creates fascinating opportunities for more extensive work in these areas.

C. THE APPROACH

This effort is intended primarily for high level decision makers who must respond to the request of the Chief of Naval Operations regarding Coast Guard DDN use. One assumption is that the reader is familiar with the basic purpose and procedures of military communications networks before the advent of the Defense Data Network. However, in an academic sense, one may also be able to gain valuable insight into state-of-the-art computer networking principles by comprehending all, or part, of this thesis. A brief description of format is presented to assist readers of either category above.

Section II contains a discussion of packet switching as it applies to the Defense Data Network. The most fundamental computer networking concepts are presented from both a physical and logical perspective. This is so the reader has a basic understanding of how DDN will accomplish its networking functions as well as outline the most elementary subscriber requirements. Section III describes the origin and extent of Coast Guard computer networks. The accent is upon the service's types of applications, data communications capabilities and overall information processing philosophy. These two sections combine to form the basis for a DDN access plan for the U.S. Coast Guard. This issue is explored from the intracommand, intercommand and interservice viewpoints in Section IV. Once the access

plan is established, the emphasis of the thesis shifts to a discussion of implementation issues. The hardware, software, and security requirements are described that can make the proposed network architecture a reality. The main focus of this Section V is on the use and determination of functional requirements and specifications. Finally, the Conclusion section outlines the overall results and observations. Here, also, an attempt is made to point out the additional development needed to transform the program plan into an operational networking scheme.

II. THE DEFENSE DATA NETWORK

A. PHYSICAL VIEW

Packet switching is the most fundamental concept used in the DDN. Figure 1 represents the structure of a typical computer-communication network [Ref. 3: p. 321]. This is by definition, an interconnection of several computers or a set of terminals connected to one or more computers [Ref. 4: p.12]. There are two basic processing operations which occur in any such network. The black circles represent switching computers called nodes (In ARPANET and DDN these are called interface message processors (IMPs). The entire collection of nodes represent the communications sub-network or backbone. This is the mechanism by which remote computer facilities exchange data. The square blocks represent HOSTS. The term host can have two meanings. DDN generally regards a host as a device that can provide access to the sub-network. In addition a host may contain the user's applications programs. The user's interface with the network is through terminals (the small open circles). Figure 1 demonstrates the various ways hosts, nodes, and terminals can be interconnected to form the network. Adjoining point to point connectors between IMPs or between hosts and IMPs are known as links. An important aspect of this type of network topology is that it relies on the store

and forward principle. Each IMP must have the ability to accept incoming data, perform internal processing and then send the information to the next processing point [Ref. 5: p.8]. The advantages of this technique will be pointed out in the discussion below of packet switching.

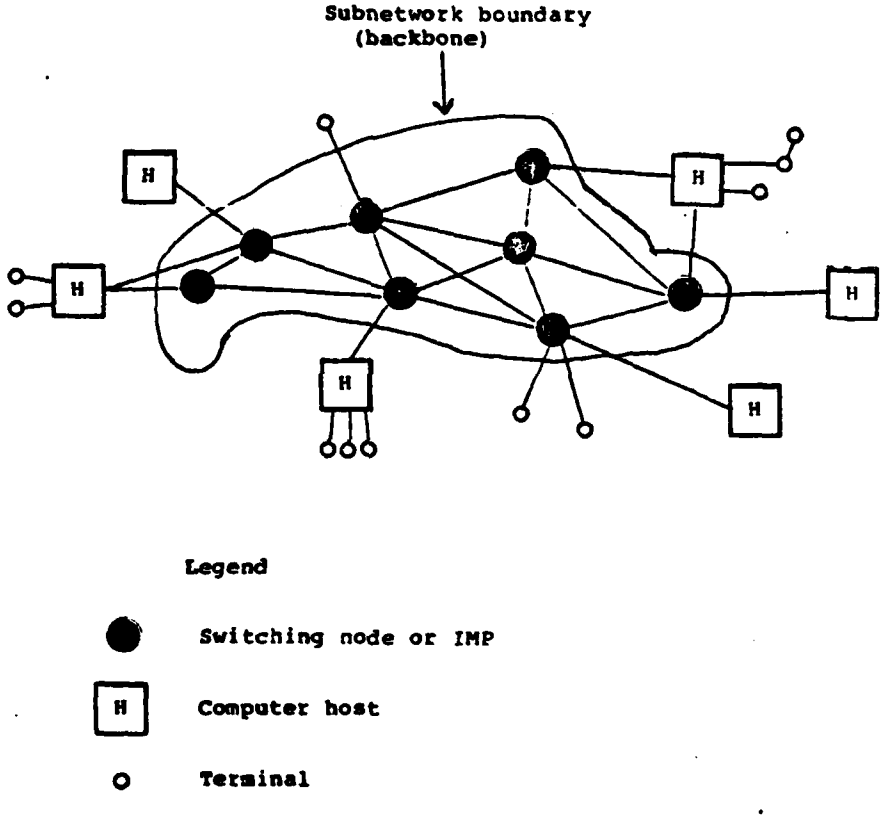


Figure 1. The Structure of a Computer Communications Network

Experience has shown that computer communications is a "bursty" process rather than a smooth flow of traffic. The beauty of packet switching is that it is not necessary to

physically establish a path, send the data stream and then close the circuit when the transmission is finished. Instead, the store and forward capability of the network can be utilized to send packets that are finite sequences of bits comprised of three main parts; a header, data and a means of error control. They are most often associated with internal subnetwork (or backbone network) operations and are not detectable to the user [Ref. 6: p. 1387]. Since each node is a programmable computer, the path a particular packet travels need not be dedicated. It is therefore possible to share network resources to the best advantage. Elaborate decisions regarding the handling of packets can be made and high speed trunks in the backbone may handle host requirements under most conditions [Ref. 1: pp. 2-3]. These advantages do not come without a price. Packet switched networks require complex routing and switching to be made. This thesis will focus specifically upon DDN network procedures. Many of these are a direct result of lessons learned from the ARPANET.

One of the basic issues in packet switching is ensuring that a packet is correctly transmitted and received between IMPS. Figure 2 is a simple model of how this is accomplished [Ref. 1: p. 2]. Each link contains an acknowledgment scheme. The receiving node analyzes, the check sum part of the packet and transmits an acknowledgment to the sender if all is well. The Defense Data network employs a sixteen bit

Cyclical Redundancy Code (CRC) for error checking [Ref. 7: p.106]. Polynominal division is performed on the checksum and a non-zero remainder implies an error. Packets are to be retransmitted whenever an error occurs. Note that the figure indicates that a switch may be called upon to handle multiple packets but that each link handles one packet at a time (with acknowledgment).

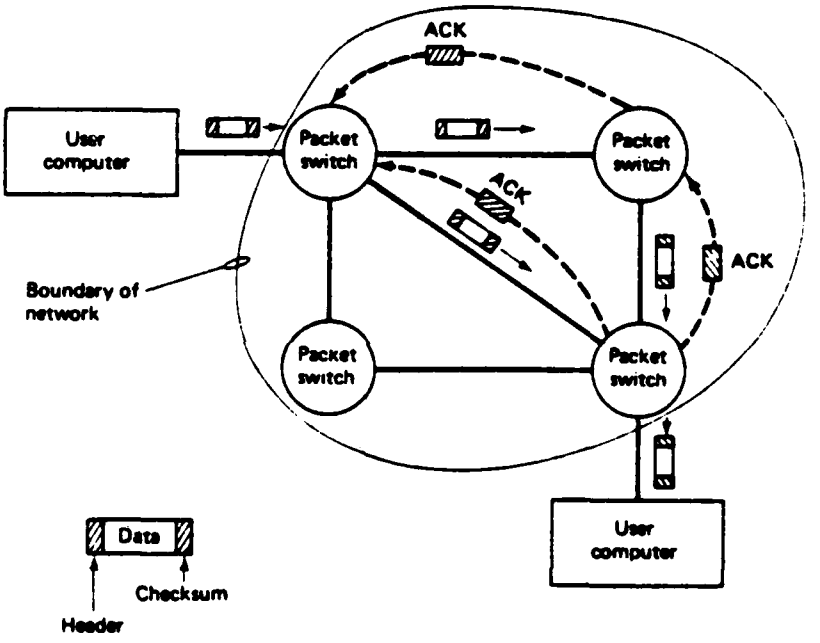


Figure 2. A Simple Model of Packet Switching

The routing of packets is another important consideration. Since each packet can move about the network independently it must contain the required address(es). This information is a part of the header. (There is a

multitude of information contained in a DDN packet header. This will be discussed in much greater detail later. Suffice it to say at this point that each packet contains, as a minimum, source and destination computer address.) There are numerous routing algorithms for networks with several improvements coming about as a result of greater experience. DDN will utilize the following type of scheme: each node will contain information on network topology and line delays. Periodically a node will measure its particular line delay and transmit this information to all other nodes. As a result each IMP will contain updated routing information and can move packets about the network accordingly [Ref. 8: p.712]. This is an example of adaptive or dynamic routing. The network attempts to change in a real-time fashion to circumvent or minimize delays.

Congestion control is also related to decreasing delay times. There are two inherent dangers to packet switched networks: 1) numerous incoming packets arriving simultaneously could flood into an IMP causing an overflow; 2) a malfunctioning IMP can overload the network with erroneous packets, preventing the flow of valid data. The Defense Data Network attempts to resolve the first problem through the use of windows and choke packets. A window is merely a specified limit to the number of send and receive sequences that a particular IMP can handle at any given time (thus preventing buffer overflow). Each node also has the

ability to reduce or cutoff the amount of incoming traffic by issuing a choke packet to its partner at the sending end of a link [Ref. 5: p.150]. A choke packet is then another internal mechanism much like the routing update packet generated for network control.

The second difficulty is handled in an easy fashion. Packets are allowed to exist in the network for a maximum of 4.25 minutes [Ref. 7: p. 179]. After this period they are automatically destroyed. Naturally there must be some mechanism to prevent the destruction of valid data. This method will be discussed in later sections.

The complete end-to-end flow of data communications is termed a path [Ref. 9: p.12]. Figure 3 points out a typical data communications path between two hosts.

The attempt of the discussion thus far has been to:

1. Introduce the concept of packet switching.
2. Understand the basic terminology and fundamentals of computer networking.
3. Provide a sample explanation of how the Defense Data Network accomplishes acknowledgment, error checking, routing, and congestion control.

Although exhaustive exposition of these topics is beyond the scope of this thesis, it will be necessary to expound on some of these ideas during the examination of the problem of connecting the U.S. Coast Guard to DDN. Of particular importance will be the addressing and other information required in packet headers. This topic is of prime importance in the sections to follow.

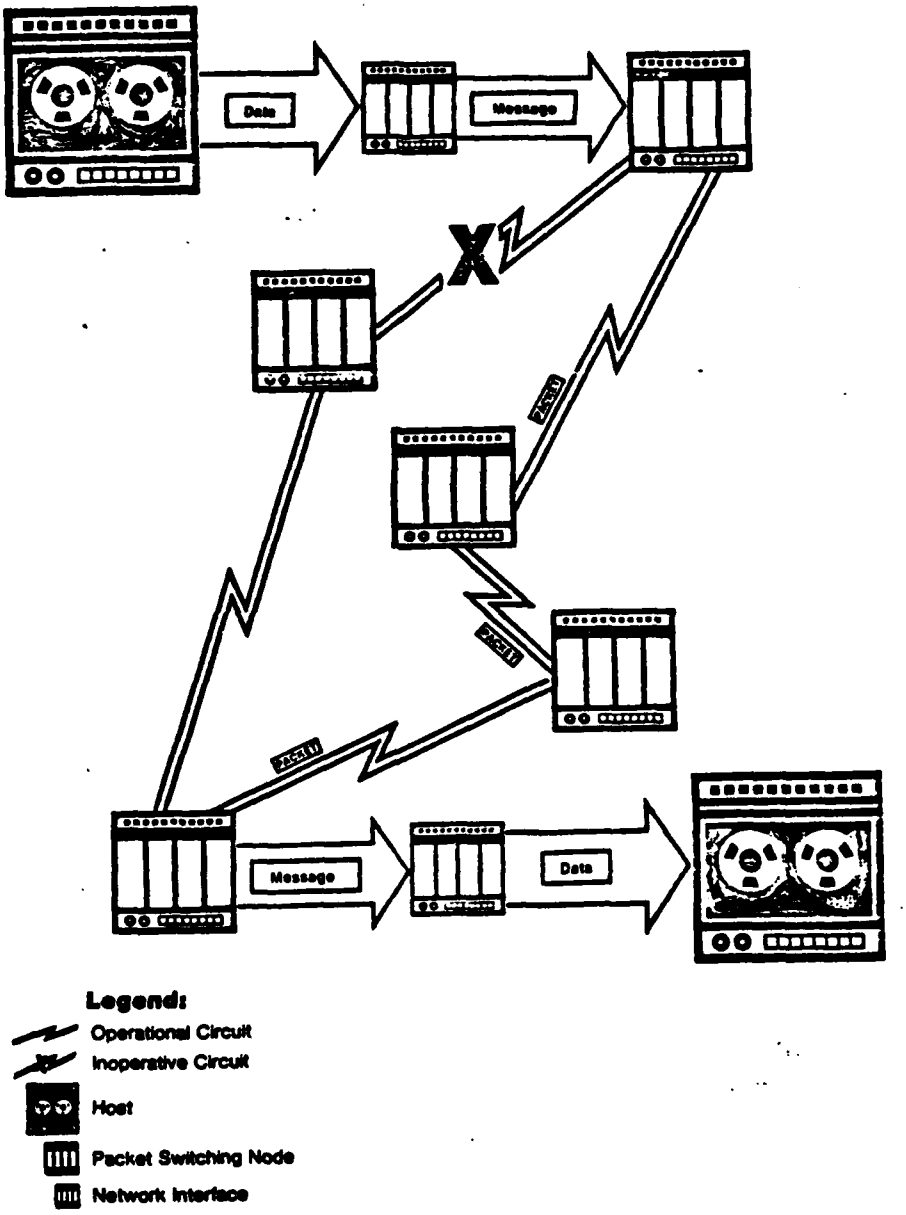


Figure 3. A Packet Switched Path Between Two Hosts

A synopsis of the physical aspects of the Defense Data Network and a description of its basic hardware components based on information contained in the Defense Data Network Program Plan, January 1982, is summarized below.

It has been demonstrated that the IMP or switching node is a key element for packet switched networks. The DDN will utilize a Bolt Barenek and Newman C/30 microprogrammed minicomputer as an IMP. The subnetwork or backbone for the initial phase (DDNI) implementation will consist of 171 of these devices located at about 85 sites as shown in Figure 4 [Ref. 7: pp.3-4].

Plans call for ninety-one subscriber systems that will consist of 488 hosts and 1446 terminals. These figures represent direct connect access only [Ref. 7: p.3].

Terminals will be able to access DDN through a unit called a mini-TAC. The mini-TAC can support up to 16 asynchronous terminals. DDNI will contain 222 of these units. (Remember in Department of Defense terminology a host is a device which allows access to the network. Mini-TACS can therefore be considered as "hosts"). [Ref. 7: p.5]

Security will be handled by two basic units, the Internet Private Line Interface (IPLI) and the KG-84 crypto device. These devices will be connected in the manner shown in Figure 5. Various key lists will be able to partition distinct user communities. [Ref. 7: pp.3-4]

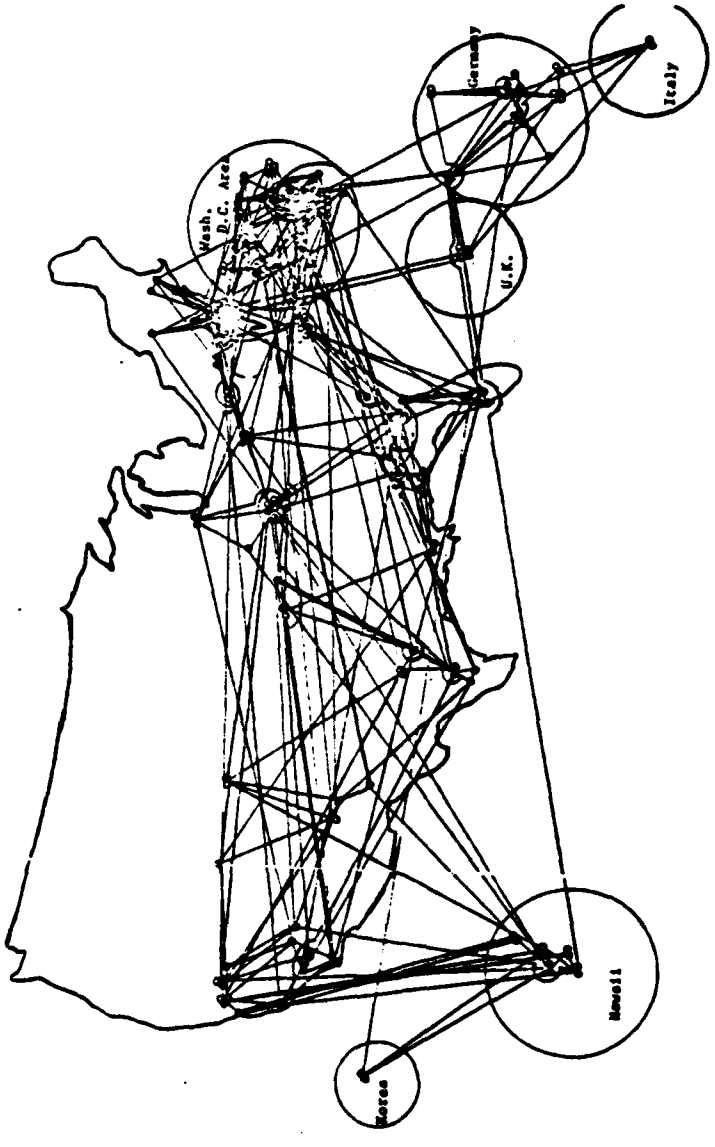


Figure 4. The Scope of the Defense Data Network

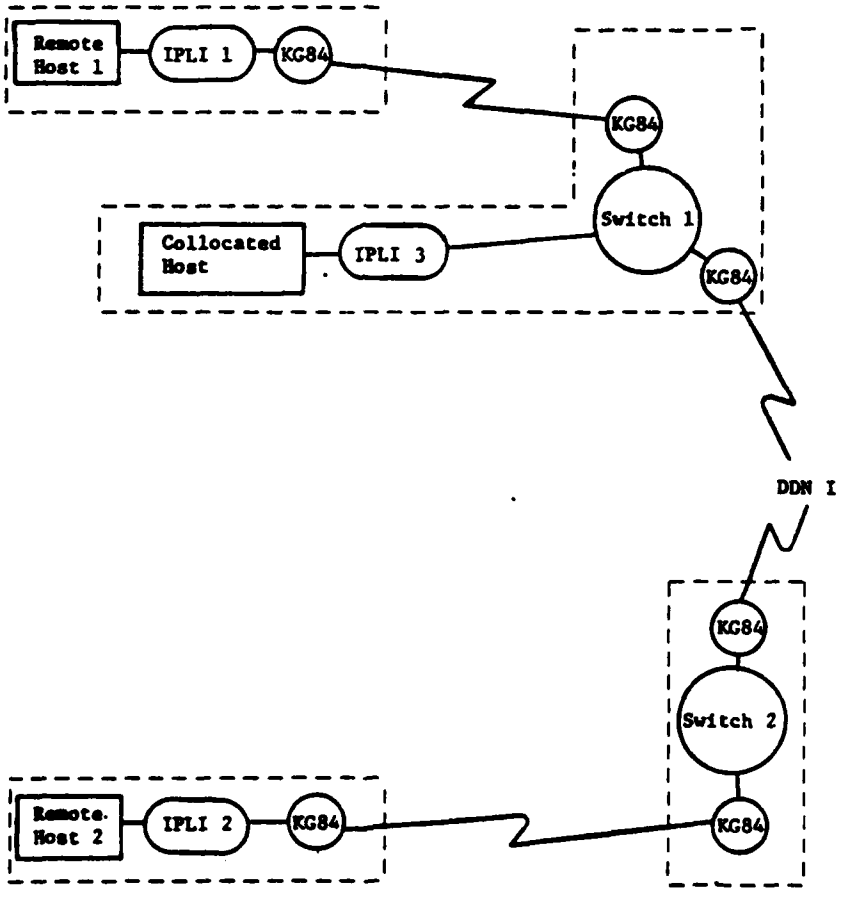


Figure 5. End-to-End Encryption

Network status is checked at Network Monitoring Centers using a BBN C/70. Sixteen operators can check the status, topology and throughput of up to 250 IMPS providing extensive network management [Ref. 7: pp.2-3].

Other possible requirements are statistical multiplexers to combine asynchronous terminal inputs and/or high speed modems to communicate via leased lines.

A cost breakdown of these hardware devices is contained in section 4.5.2 of the DDN Program Plan and is presented as Appendix A.

B. LOGICAL VIEW

Computer networks are much more than a set of interconnected black boxes. There are several key ingredients that have yet to be addressed. Perhaps the most basic issue is the method for transmitting packets throughout the network. Three distinct processes are in fact involved to accomplish this goal. First, there must be an access process to gain entry into the sub-network. Second, a communications process is required between the nodes forming the sub-network and third, end to end control is required since packets may travel over a variety of paths to reach their final destination. To complicate matters further, consider that the end user often desires to transfer application files to a computer that has a different operating system, file structures, etc. from that of the

originator. It would be impossible to resolve these problems with a single hardware/software package. Network designers have instead opted for a layering approach, that is breaking down the total communications function into a hierarchical set of modules. This closely resembles a top down design approach to software design.

The International Standards Organization (ISO) has defined seven layers for computer networking. The layer names and a few examples of their functions are presented in Table I [Ref. 10: p.131].

Table I. The Seven International Standards Organization Layers

LAYER	EXAMPLES OF FUNCTIONS
APPLICATION	FILE TRANSFER/MAIL/TELNET FILE UPDATE/DBMS
PRESENTATION	CODE CONVERSION/FORMAT CONVERSION
SESSION	CONNECTION OF COMMUNICATING PARTIES
TRANSPORT	RELIABLE IN-SEQUENCE DATA TRANSMISSION
NETWORK	ROUTING
LINK	FLOW CONTROL/ERROR CONTROL
PHYSICAL	PIN LAYOUT/VOLTAGE LEVELS/ RISE TIMES

Figure 6 illustrates how two computers with user applications packages can communicate using the ISO model.

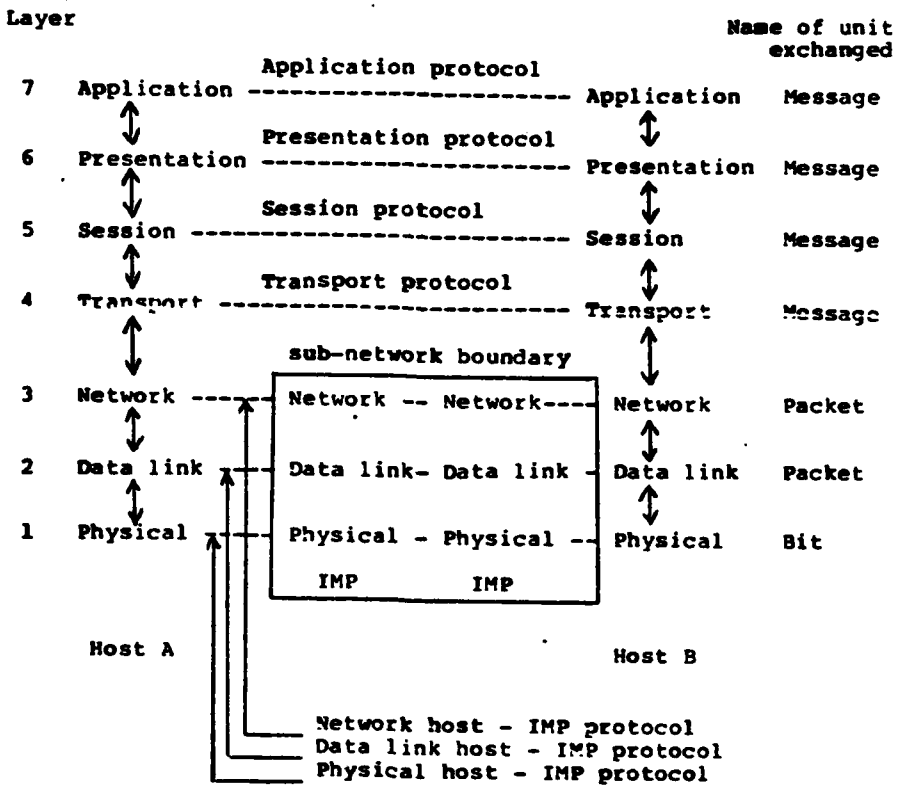


Figure 6. The Interaction of Protocols Within the ISO Model

[Ref. 5: p.16] There are several points of interest here. Notice that vertically, each layer relies directly on the layer below. Horizontally, only the physical layer deals with the physical transmission of data. All other communications are virtual. That is, in the higher layers there are no physical transmission lines. Instead, protocols are used to give the impression of a connection between the two hosts at each layer. A protocol can be defined as a set of conventions or rules that allow two end

points to communicate [Ref. 6: p.1387]. These end points may be physical in nature or they may deal entirely with the logical layering process described above.

There are two methods by which packets may travel through a network called virtual circuit and datagram. A virtual circuit is a logical channel between the source and destination. An initial setup is required and packets are delivered in the order sent [Ref. 11: pp. 501-502]. A virtual circuit is analogous to a typical telephone conversation. The caller dials a phone number and a set-up phase (connection establishment and ringing) is involved. When the receiver picks up his phone, voice data is transferred in a sequential manner until the connection is closed (hang-up). [Ref. 5: p.188] On the other hand, in a datagram type of service, individual packets travel unacknowledged in simple units throughout the sub-network. Packets may arrive at the destination in an unsequenced fashion. There is no set-up phase in a datagram service [Ref. 5: p.189]. A datagram can be compared to a letter in the postal system. Each correspondence is an isolated, addressed entity. [Ref. 5: p.189]. The differences between virtual circuit and datagram services is given in Table II. The key issue is to delineate the function of the host from those which should reside in the sub-network.

The controversy as to which method is preferred in computer networks rages on. It would appear that the short

Table II. The Differences Between a Virtual Circuit and a Datagram

Issue	Virtual circuit	Datagram
Destination address	Only need during setup	Needed in every packet
Error handling	Transparent to host (done in the subnet)	Explicitly done by the host
End-to-end flow control	Provided by the subnet	Not provided the subnet
Packet sequencing	Messages always passed to the host in the order sent	Messages passed to the host in the order they arrive
Initial setup	Required	Not possible

"burstyness" of computers would lend itself more favorably to datagrams. However the sequential nature of communication between sender and receiver suggests that virtual circuits should be used. Notice also that the differences between the two call for a corresponding difference in the layering process. Virtual circuit service corresponds more closely to the ISO model [Ref. 12: p.128]. Originally the ARPANET was also designed as a virtual circuit model. [Ref. 5: pp.369-370] However, DARPA later came to realize one major advantage to datagrams. Individual packets could simultaneously be transmitted throughout the sub-network over numerous channels. This combined with the fact that set-up time is eliminated

offered tremendous speed advantages. Consequently, an effort was begun that would depart from traditional ISO philosophies in networking. Through the implementation of two new protocols called the Internet Protocol (IP) and the Transmission Control Protocol (TCP), the ARPANET was successfully able to establish a datagram type of service in the sub-network (backbone) while providing sequencing in the higher transport layer.

Meanwhile industry, (particularly the international community) developed a virtual circuit protocol called X.25. This protocol is entirely compatible with the physical, data link, and network layers of the ISO model [Ref. 11: p.508]. There are also provisions for datagrams in X.25 but commercial availability of this service is extremely limited [Ref. 1: p.125].

The Department of Defense believes that military requirements dictate the need for both datagram and virtual circuit services [Ref. 12: p. 127]. The Defense Data Network will eventually support X.25 as well as TCP and IP. Nevertheless, DDN is doing everything in its power to promote international acceptance of the datagram-based TCP and IP protocols [Ref. 13: p.116]. In fact, access to the network will be denied without their installation. These form the basis of invoking the remote job entry and file transfer protocols at a higher level.

The consequences of this decision are of profound importance to those attempting to utilize DDN. The Defense Data Network is not a homogeneous means of interconnecting computers. Rather, it is a bold effort designed to interface numerous network communities. Communications between hosts can be a result of any of the following:

1. simple bus structures.
2. virtual circuits (particularly X.25).
3. ARPANET (TCP, IP).
4. local area techniques (e.g., Ethernet).

The DDN proposes to be compatible with each of these methods.

The challenge of this thesis is quite clear and rests in three parts. First there is a need to examine the networking capabilities of U.S. Coast Guard computer resources. Next an understanding of the hierarchical process of connecting local networks to DDN is required. Finally, the functional requirements to achieve this interconnection must be developed (particularly in the area of required protocols). Only then can a comprehensive program plan for the access and utilization of the Defense Data Network by the U.S. Coast Guard be developed.

III. COAST GUARD COMPUTER NETWORKS

A. OPENING REMARKS

As little as ten years ago, the U.S. Coast Guard relied almost solely upon traditional military communications schemes to meet the service's networking needs. Radio nets, the telephone and hard copy teletype message traffic were the command and control mechanisms to fulfill both operational and administrative mission requirements. During the early seventies, the Coast Guard began to realize the advantages of data-based management information and decision support systems. Consequently, several specialized computer networks were developed by various communities of interest that were designed to perform unique mission functions. Four long haul networks classifications emerged from this effort. They are:

1. Operational Networks (Search and Rescue, Law Enforcement).
2. Marine Safety Networks (Vessel Documentation, Licensing).
3. Administrative Networks (Personnel and Finance).
4. Traditional Telecommunications Networks (Autodin).

In addition, numerous mini/micro computer local area networks (LAN) sprang up to meet the word and data processing needs at the unit level.

This section will describe the primary network in each of these categories. A knowledge of the Coast Guard's organizational structure may be required to understand the rationale behind interconnections. Table III is included for this purpose. One assumption is that the operational requirements for these systems have been predetermined. Therefore, issues that deal specifically with data content or the inclusion/exclusion of a particular node will not be discussed here. The main focus is on a functional interconnection approach and not the exact content of computer telecommunications.

B. OPERATIONS COMPUTER CENTER (OCC)

The Operations Computer Center is a centralized, real-time information processing resource designed to provide data base access or run sophisticated computer programs. Here is a listing of some of the services provided by the OCC [Ref. 14: pp.1-9]:

1. Computer Aided Search Planning (CASP)-A mathematical model for computer assisted search planning.
2. Automated Mutual-assistance Vessel Rescue System (AMVRS)-A means of providing worldwide ship movement tracking.
3. Operations Information System (OPINS)-A operational information and resource inverting system.
4. Search and Rescue Satellite Aided Tracking (SARSAT)-self explanatory.

TABLE III

A BRIEF OUTLINE OF THE TYPES OF COMMANDS FOUND IN COAST GUARD LONG-HAUL NETWORKS

ORGANIZATIONAL UNIT	MISSION DESCRIPTION	EXAMPLE
Headquarters	Highest organizational level in the Coast Guard. Dictates service wide plans and policy.	CGHQ DC
District Office	Subordinate to Coast Guard Headquarters. Responsible for Coast Guard operations within a geographic area.	CCGD Thirteen Seattle
Communication Station Radio Station	A unit that provides communications support, usually to larger floating platforms.	NMA Radsta Miami
Computer Resource Unit	Commands which have large computer mainframes and specialized data bases.	AMVER New York
Autodin Switching Centers	Major nodes for the Autodin system.	McClellan

Redundant Prime 750 minicomputer systems are utilized for the above purposes at a facility located at Governors Island, New York. The OCC has X.25, Telenet, and Primenet tele-processing system software for networking. Most subscribers to the OCC use the commercial Telenet dial-in capability to communicate with the Prime mainframe. Figure 7 points out the principle trunk lines of Telenet [Ref. 15: pp. 11-14]. Since this network is largely oriented toward search and rescue, the main users are Coast Guard District Command Centers who dispatch rescue resources. In addition to the services mentioned above, each District has a reserved data storage space where unique application packages may be developed.

C. MARINE SAFETY INFORMATION SYSTEM (MSIS)

When completed the Marine Safety Information System will be a nationwide, comprehensive data base system with over 180 different data files dealing with commercial vessels, their owners and activities. MSIS will provide real-time information concerning, licensing and documentation [Ref. 14: pp. 1-9, 1-10]. A basing plan for seven MSIS mini computers has yet to be fully developed. However, an interim network has been established using primarily Coast Guard units along the Gulf Coast. Figure 8 outlines the extent of the initial MSIS network [Ref. 15: p. 9-6].

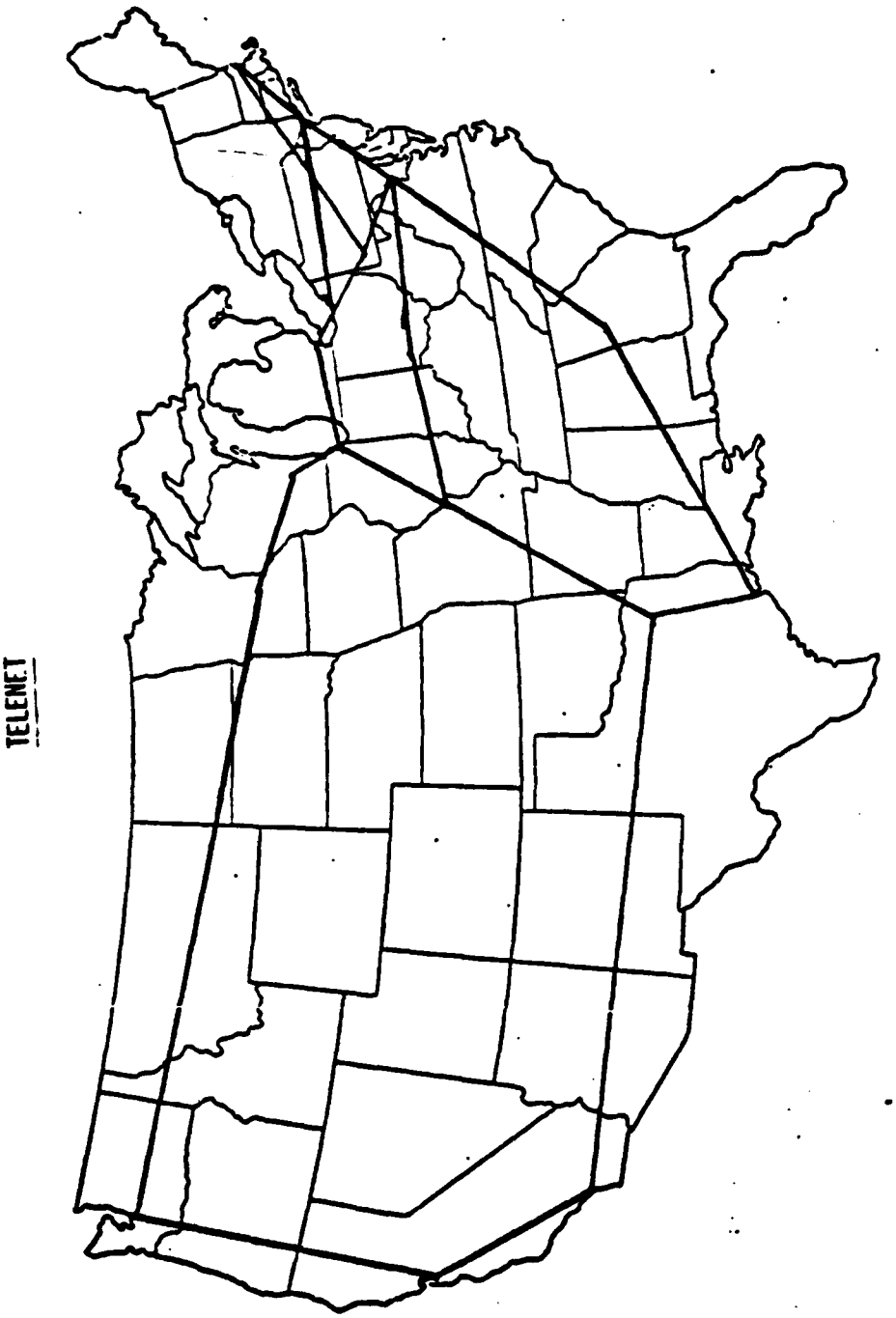


Figure 7. TELENET

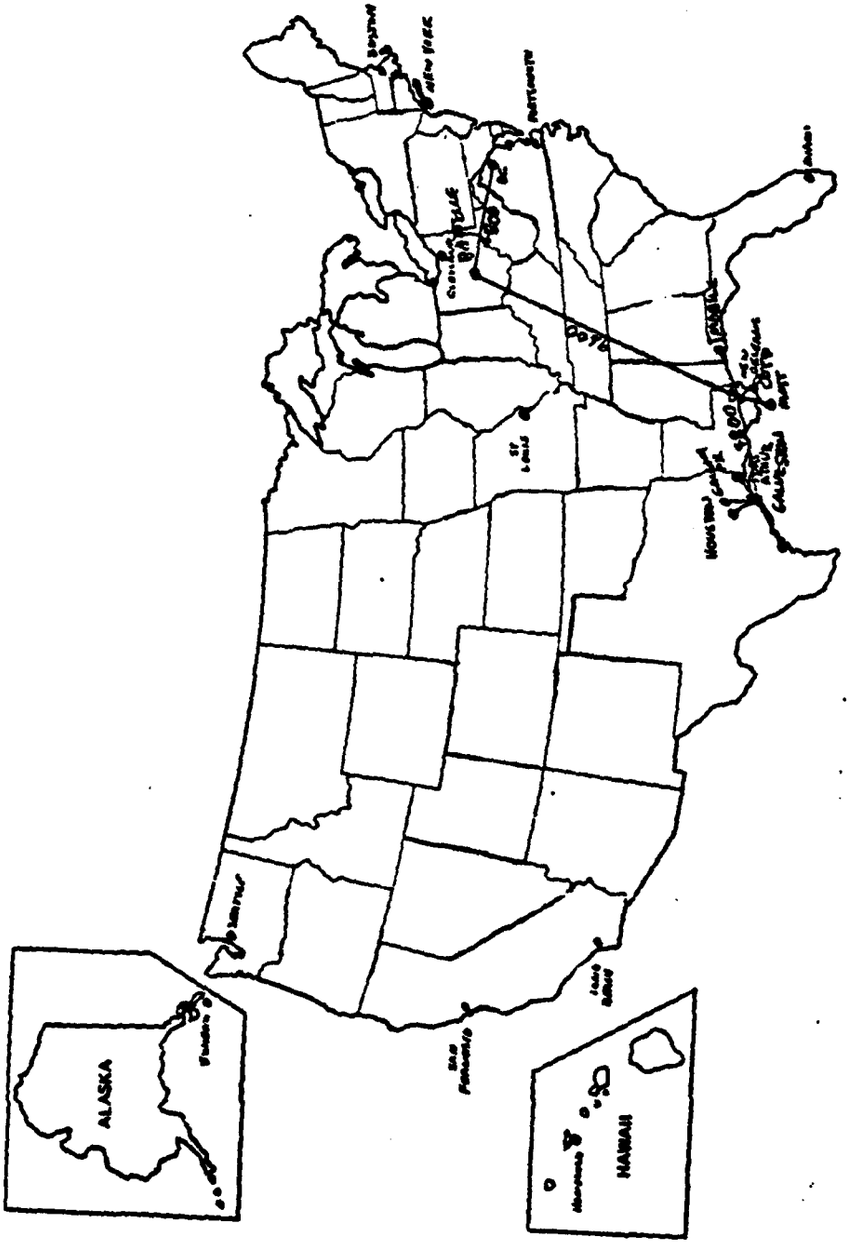


Figure 8. The Interim MSIS

The MSIS is also currently invoking Telenet's public data network for telecommunications services. It is therefore quite possible for some commands to access the OCC and MSIS with equal ease. The only requirement is a real need to tie into these data bases. MSIS promises to become the most extensive long-haul network in the Coast Guard.

D. ADMINISTRATIVE SYSTEMS

There are two major categories of administrative computer systems in the Coast Guard. Transactions are usually oriented either toward personnel and/or supply matters and are conducted using the Personnel Management System (ARMS) respectively. Each of these systems will be discussed in further detail.

PMIS maintains a master file of all Coast Guard active duty and reserve personnel. Data items include name, rank, training, qualification codes, etc. During June of 1983 the Coast Guard implemented a revised PMIS network. Microprocessors equipped with X.25 telecommunications software have the ability to access the extensive personnel data base from larger mainframes. This marks the first occasion where the Coast Guard may choose to invoke both the X.25 protocol and distributive processing on a large scale basis (the physical and logical attributes of this type of connection will be discussed in Sections IV and V). PMIS

and supply data can be handled in a very similar fashion. In fact, the same mainframes often control both data bases.

The development of ARMS closely parallels PMIS. The purpose of ARMS is to provide supply personnel with an automated system for requisitioning supplies as well as monitoring the status of open requisitions. This will eliminate the need for numerous hardcopy ordering forms used in the past.

PMIS and ARMS are the major components of a network loosely called the Information System by the Coast Guard. Figure 9 shows the nodes and line speed of this network [Ref. 15: p. 9-5]. The Information System are organizational units comprised of Coast Guard Headquarters, all district offices and the Military Pay Center. Eventually it will handle nearly all of the service's administrative matters requiring computers. The key to the success of this venture is in the ability of minicomputers at each node to download interactive applications file packages to microprocessors. The first attempt at this is, of course, PMIS as mentioned earlier.

E. TRADITIONAL TELECOMMUNICATIONS

The Coast Guard is in a unique position with regard to the handling of military message traffic. During peacetime this service is not a part of the Department of Defense and often employs non-DOD radio and teletype

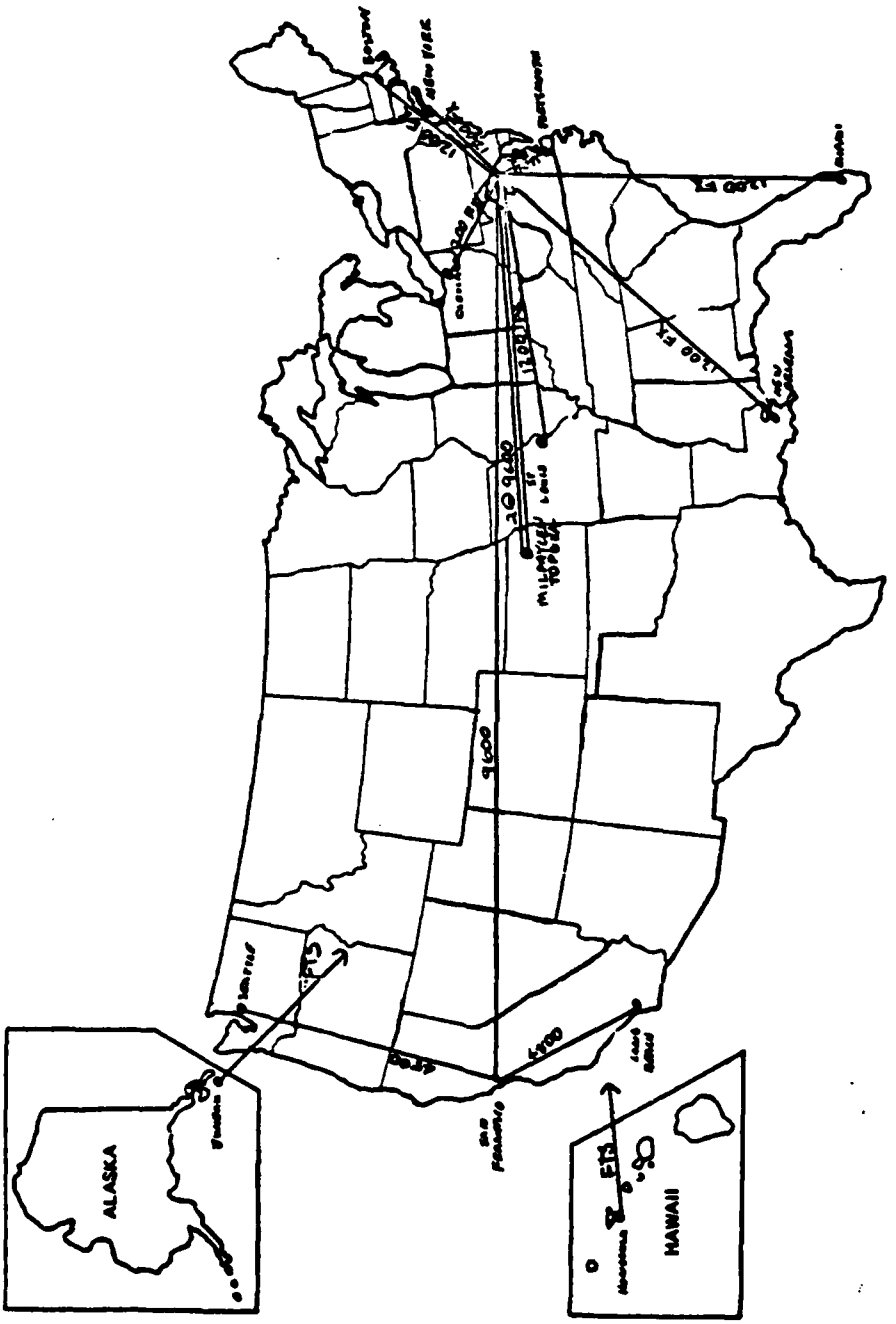


Figure 9. The Information System Network

networks. However, the Coast Guard does become a part of the Department of the Navy during wartime and thus must maintain full compatibility with Naval communications systems. The result has been the formation of two principle long haul telecommunications networks. On the one hand the Coast Guard is currently a part of DOD's worldwide Autodin system and at the same time it is in the process of developing an intraservice Operational Digital Network (ODIN). Each of these merit further explanation.

Figure 10 shows the Coast Guard's Autodin Access and Table IV gives a brief outline of the status of Autodin installations [Ref. 15: pp. 9-1, 9-4]. Almost all Autodin hardware and software is provided to the Coast Guard through arrangements made by the U.S. Navy. In turn, the Coast Guard meets the receiving costs of operating their installations. Since the Defense Data Network will replace Autodin and compatibility must be maintained, it is certain that, at the very minimum, the sites listed in Table IV will be granted DDN access. Autodin has been described as the Coast Guard's record message workhorse [Ref. 14: p. 1-7]. This was because intra-service message networks consisted of slow (100 baud) teletype loops. It was often faster to use Autodin to route traffic between Coast Guard Commands that had access to the DOD network. Another constant necessity is to relay messages by converting from Coast Guard teletype to Autodin and vice-versa. Currently, this means a change

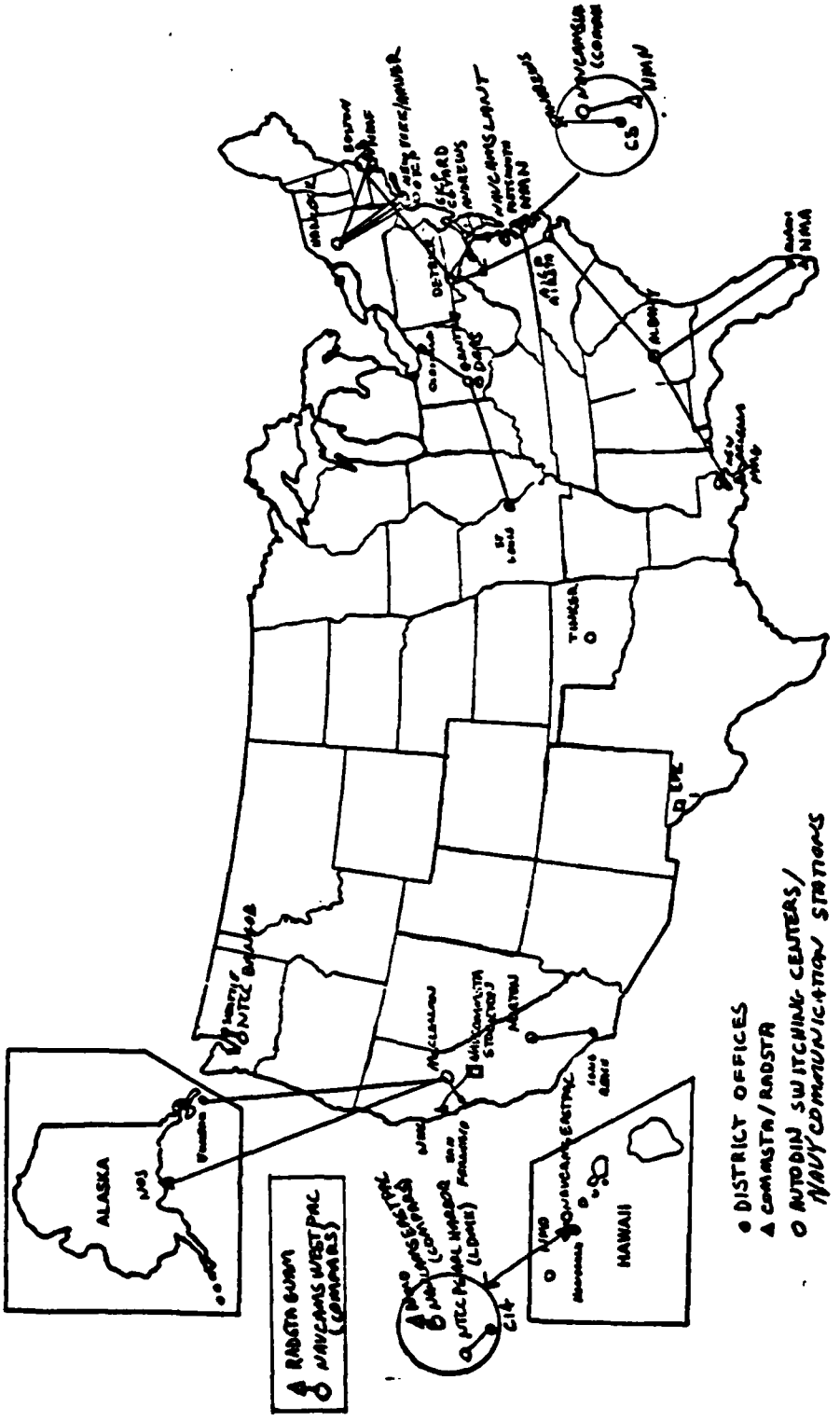


Figure 10. AUTODIN Access

Table IV. Current Status of Coast Guard AUTODIN I Installations

RI	UNIT	SERVICE	ASC	REMARKS
RUEOABA	CCGDONE	MODE I SRT II 300 BAUD	FT DIETRICK	
RUCIHLA	CCGDTWO	MODE V 75 BAUD	GENTILE	TO BE REHOMED TO SCOTT AFAMPE FY82
RUEDEEA	CCGDTHREE	MODE I SRT II 300 BAUD	HANCOCK	
RUEBESA	CCGDFIVE	MODE I SRT II 300 BAUD	ANDREWS	
RUCLFOA	CCGDSEVEN	MODE I SRT II 300 BAUD	ALBANY	
RUCLFWA	CCGDEIGHT	MODE I SRT II 300 BAUD	ALBANY	RIXT B IN FY83
RUCIAEA	CCGDNINE	MODE I SRT II 300 BAUD	GENTILE	
RUWJNJA	CCGDELEVEN	MODE I SRT II 300 BAUD	NORTON	
RUWMHIA	CCGDTWELVE	MODE I SRT II 300 BAUD	McCLELLAN	
RUWMFUA	CCGDTHIRTEEN	RIXT B	VIA LDMX NTCC BANGOR	
RUHMAGA	CCGDFOURTEEN	RIXT B	VIA LDMX NTCC PEARL HARBOR	
RUWMDMA	CCGDSEVENTEEN	MODE V 75 BAUD	McCLELLAN	
RUEDQNA	GICP	MAID 300 BAUD	HANCOCK	
RUEBQWA	SICP	MAID 300 BAUD	ANDREWS	
RULLQLA	AICP	MAID 300 BAUD	ALBANY	
RUEDEPA	COMMSTA BOSTON	MODE I 150 BAUD	HANCOCK	MODEL 37 TTY INTERFACE
JLYWCA	COMMSTA PORTSMOUTH	NAVCOMPARS	VIA NAVCAMSLANT NORFOLK	
-------	RADSTA MIAMI	NONE		MODE V WAS TO HAVE BEEN INSTALLED IN FY80. PENDS
-------	RADSTA NEW ORLEANS	NONE		
RUWNSJA	COMMSTA SAN FRAN	NAVCOMPARS	VIA NAVCOMMSTA STOCKTON	
RUHPGIA	COMMSTA HONOLULU	NAVCOMPARS		
RUEGJAA	RADSTA GUAM	UNCLAS NAVCOMPARS	VIA NAVCAMS WESTPAC	
RUWMEBA	COMMSTA KODIAK	MODE V 75 BAUD	McCLELLAN	
RUEOBGA	AIRSTA E CITY	MODE V 75 BAUD	FT DIETRICK	
RUEBLJA	GROUP BALTIMORE	MODE V 75 BAUD	ANDREWS	
RUEDAYA	AMVER	MODE V 75 BAUD	HANCOCK	TO BE UPGRADED TO MODE I
RUEBASA RUEBJGA	CGHQ	MODE V 75 BAUD	ANDREWS	TO BE UPGRADED TO RIXT B VIA NTCC CRYSTAL CITY

in routing format and the cutting of a paper tape. Unfortunately, the only interface between Autodin and intra-service teletype is via paper tape. One of the main obstacles of automatic switching is that the majority of Coast Guard teletype circuits are unclassified. This presents a real security danger when classified traffic is destined to Coast Guard commands through Autodin.

The outgrowth of the above situation was plans for the establishment of ODIN. It was obvious that there are two major problems with the message handling system as it presently exists. First, intra-service networks were slow and constantly congested. Second, the paper tape relay process is extremely labor intensive. ODIN is a 1200 baud, polled message system. Figure 11 outlines the extent of the ODIN network. The circuits along the Atlantic Coast have already been installed and are operational. When completed, ODIN is to become the Coast Guard's primary means of handling intra-service message traffic [Ref. 15: p. 5-1]. The system relies upon microprocessor technology to accomplish polling, routing, header conversion, etc. One additional objective of the ODIN project is to develop an interface unit between ODIN and Autodin (even though Autodin is to be replaced, it is necessary to link Coast Guard and DOD networks by some means other than paper tape). ODIN is an unclassified communications scheme. Plans are to establish the Secure Command and Control Network (SCCN) to

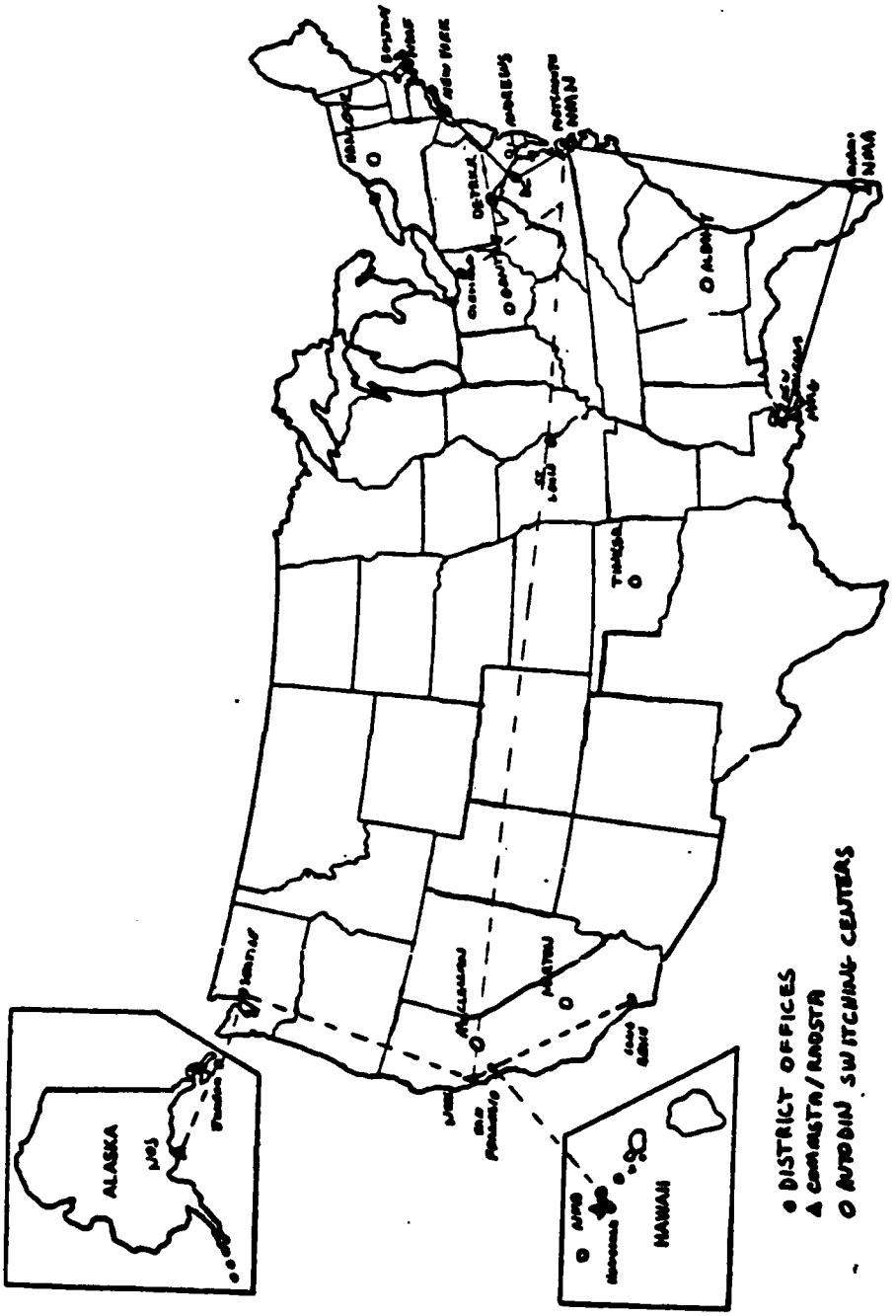


Figure 11. The ODIN Network

become the primary means of processing classified messages in the Coast Guard. Figure 12 shows the interconnections of SCCN [Ref. 15: p. 9-3]. Together ODIN and SCCN will provide a means for the service to handle all message traffic by automatically routing to the appropriate communication network(s).

F. COAST GUARD LOCAL AREA NETWORKS

The decreasing cost of hardware has made it advantageous for even the smallest commands to possess some form of computer processing capability. One natural outgrowth of this is the desire to the computer resources together. This is true not only in the long-haul networking sense but also on a localized level.

The Coast Guard recognized this need for all units to acquire this standalone processing ability and at the same time have the option to perform networking. Recent advances in microprocessor design made this idea a worthwhile proposition. In order to ensure compatibility the service focused on a large scale acquisition of one thousand microcomputers by the same manufacturer. The desire was to purchase devices with a sizable internal capacity and extensive communications ability. For obvious reasons, this effort became known as the Standard Terminal project. During June of 1981 a vendor known as Convergent

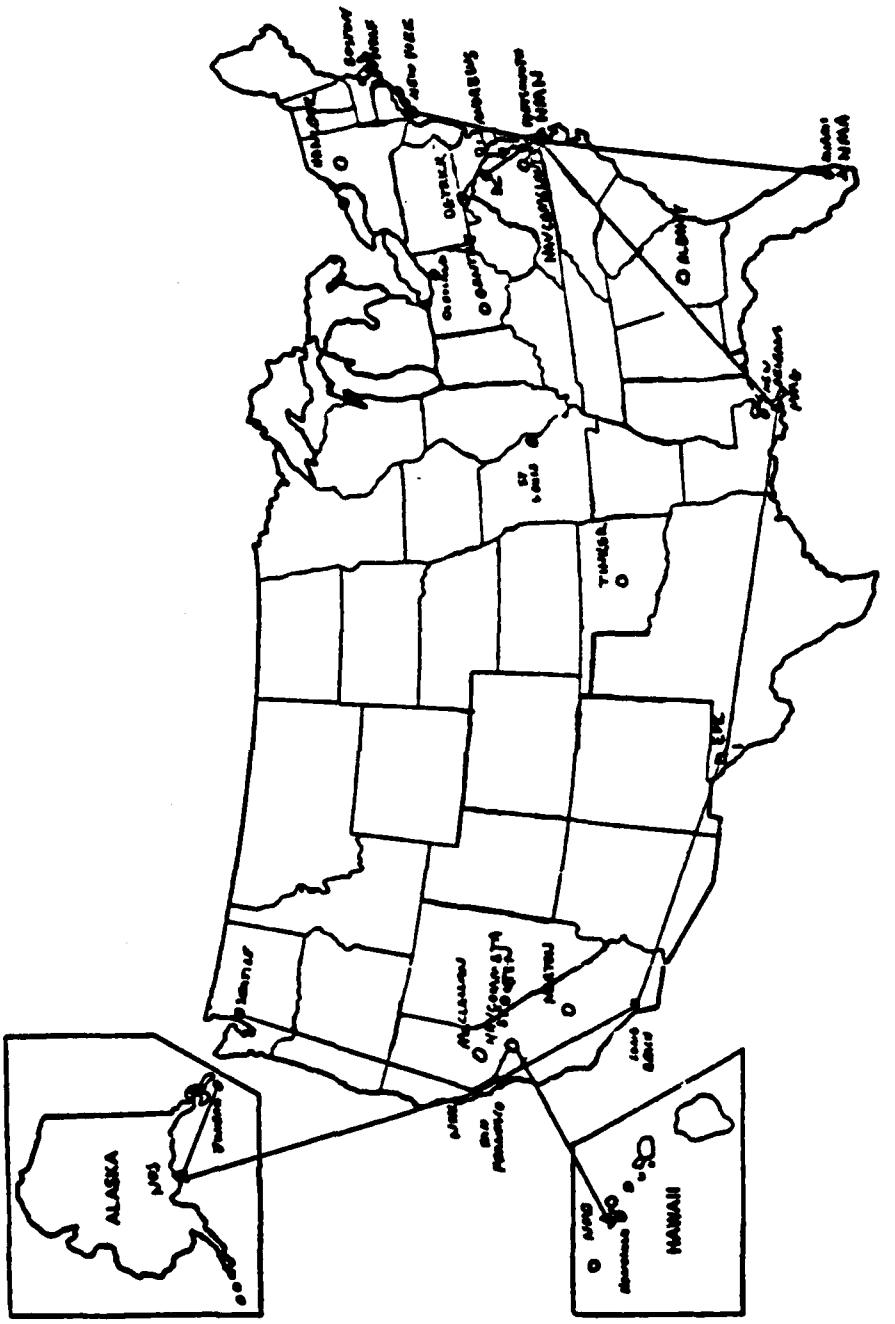


Figure 12. The Secure Command and Control Network

Technologies or C3, Inc., was chosen to provide the Standard Terminal [Ref. 14: pp. 3-19].

The Standard Terminal is a sixteen bit microcomputer with one megabyte of internal storage. It supports numerous high order languages (i.e., Pascal, Fortran, Cobol) as well as word processing, graphics and specialized applications programs. One of the strongest features of the Standard Terminal is in the area of communications. Up to sixteen terminals may be clustered to form a local area network bus structure. The unit also supports all three levels of X.25 protocol (physical, data link, and network layers of the ISO model) for long-haul networking. In addition, the Standard Terminal may be made to emulate nearly any asynchronous terminal device. These features have proven invaluable to the Coast Guard. This microprocessor is the basic component of the PMIS and the principle terminal device for communicating with OCC, MSIS and other mainframes. The unit may also serve as a teletype replacement under ODIN. The Standard Terminal has also been used to access a Defense Data Network TAC at the Naval Postgraduate School.

The use of the Standard Terminal is local area networking varies from place to place. Some districts have the ability to download applications from a minicomputer to Standard Terminal networks. Other commands are using clustered terminals without connecting to a larger mainframe. Still others invoke the Standard Terminal in a

stand alone mode or simply use it as a "dumb" terminal to connect to the systems described in this Section via Telenet.

G. THE NEED FOR AN INFORMATION ARCHITECTURE

Each of the computer processes outlined evolved from separate communities of interests to meet unique needs. Consequently, the networks that supported these applications also arose independently. The Coast Guard can no longer afford to pursue computer host telecommunications in this manner. The service has begun to realize that the various networks are simply resources that move and process data, regardless of whether the information itself is supply, personnel, operational or military message traffic in nature [Ref. 14: p. 1-1]. Therefore, the need is to develop a comprehensive information architecture to allow different parts of the Coast Guard to implement applications at different paces. The issue then becomes an overall network management task to ensure transactions are handled with the appropriate connectivity security and priority. Figure 13 outlines this planned information architecture approach [Ref. 14: p. 1-2].

Historically there has been a district split between traditional record communications and data communications. The user of the Coast Guard's Communications System was the communicator per se. The rise of computer networking has

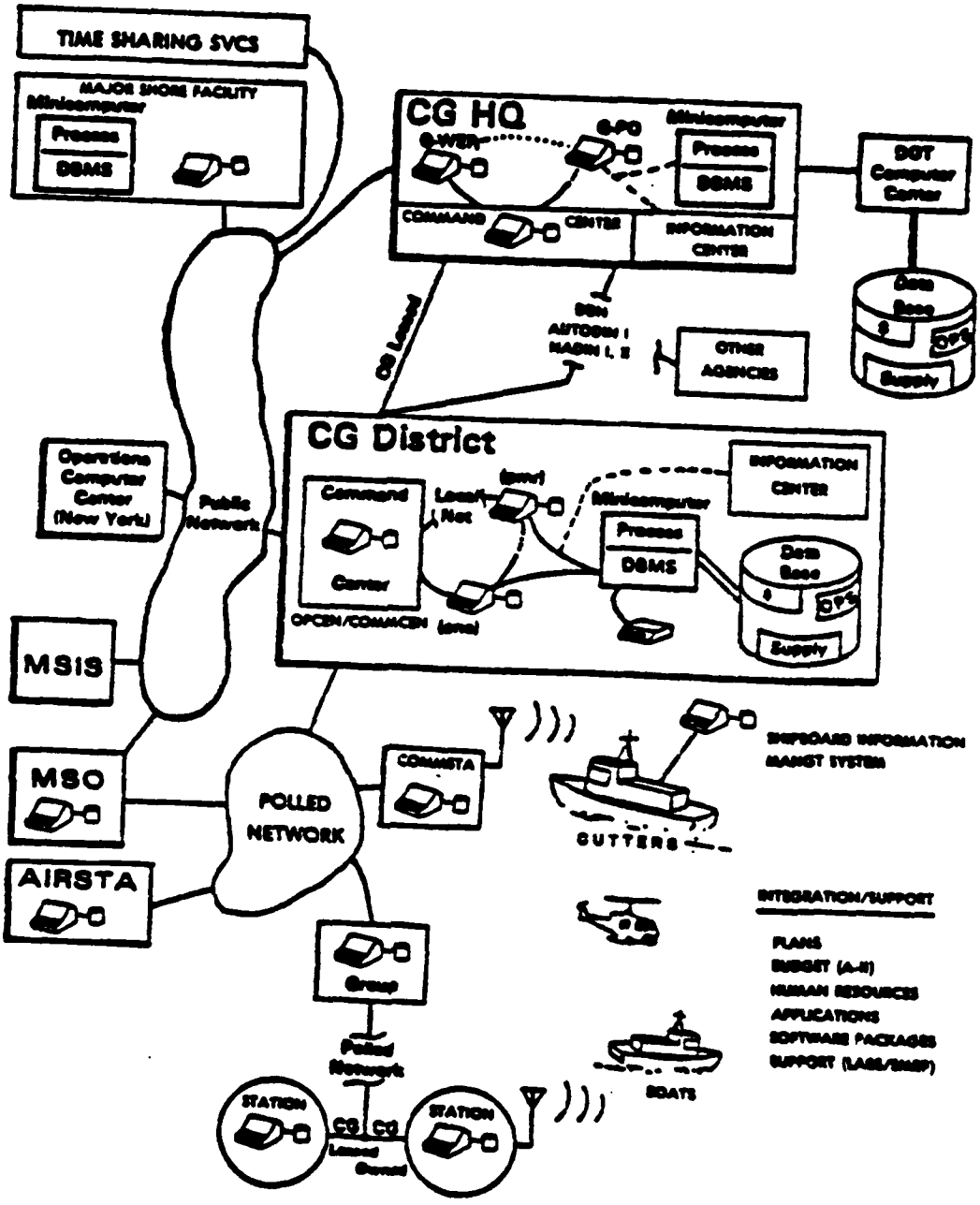


Figure 13. Coast Guard Information Resources Management Architecture

changed this philosophy. The user is actually the person or program processing an application. The network manager then becomes a facilitator or change agent for users [Ref. 14: p. 1-1]. The Defense Data Network has also adopted this approach. Although DDN will replace the entire Autodin system, it is estimated that over seventy percent of the communications on the network will contain computer data, not record message traffic [Ref. 7: p. 67].

One of the major unanswered questions is exactly what role DDN will play in the Coast Guard's Resources Management Architecture scheme. Figure 13 shows DDN as a link between Coast Guard Headquarters, District and other agencies, but the functional requirements for this connection have yet to be determined. This illustration also points out that the service's efforts have been in the areas of public networks (Telenet) and polled networks (ODIN). Under the arrangement illustrated, each District would be required to maintain the hardware and software for four separate long-haul networks. This implies tremendous compatibility and relaying problems as well as the need for a variety of resources. It would certainly be advantageous to lessen this difficulty by placing more systems on fewer networks. The logical choice would be to expand DDN access and thereby eliminate the need for other means of computer telecommunications because:

1. The Coast Guard will require DDN access to be compatible with DOD.

2. DDN is designed to provide effective computer host telecommunications that is based on the success of ARPANET.

3. Commercial carrier services are expensive and may not meet the security needs of the Coast Guard.

4. Intra Coast Guard and DOD record communications networks should be automatically interfaced.

5. It is quite likely that the U.S. Navy will provide much of the DDN hardware in an arrangement similar to Navy/Coast Guard Autodin agreement.

The advantages to this perspective do not come without paying a price. The Coast Guard would be forced to abandon many installed and planned networks and accept the packet switched, datagram-based model described in Section II. It would also be impractical to give every Coast Guard unit direct access to DDN. Some form of intra-service communications must be maintained. It is important to note that the Coast Guard is not a major DDN subscriber. The other services will require the vast majority of resources. On the other hand, it is foolish to merely replace every Autodin terminal with DDN hardware. The need to merge data and record communications is known by all parties.

The next sections will attempt to consolidate the physical and logical aspects of DDN with the needs of the U.S. Coast Guard. The focus will be upon determining DDN access and developing the functional requirements necessary to grant that access. The boundaries between intra-service

networks and the Defense Data Network could be anywhere along the Coast Guard's organizational hierarchy. Figure 13 suggests that District offices and computer resource units are prime candidates for consideration of the placement of the boundary. This means that the majority of the discussion will center upon linking local area networks and larger Coast Guard communities of interest to DDN.

IV. RECOMMENDED DDN ACCESS PLAN

A. PURPOSE

The purpose of this section is to determine the level of Defense Data Network access by the U. S. Coast Guard. The recommendations presented herein are based upon two criteria. First, DDN access should only be granted to computer hosts that meet the Defense Data Network's design objectives. There is little value in going through the expense of adopting the packet switching techniques of Section II when no real need for host telecommunications is present. The second consideration is that Coast Guard DDN access must be consistant with the information resources management architecture presented in Section III. The Defense Data Network must be an integrated part of the Coast Guard's total networking scheme. It is of paramount importance that existing systems become adaptively compatible with DDN to avoid the cost and effort of maintaining multiple, specialized network structures.

The process of examining each Coast Guard command individually to decide if the above criteria are met would be a laborious task that may not produce the desired results. A better approach is to view the access question from the intracommand, intercommand and interservice perspective. Many commands can utilize the Coast Guard's

computer systems in exactly the same manner with geographic location being the only difference.

B. INTRACOMMAND ACCESS

Intracommand access implies the use of DDN for data communications between locations within a single unit. This is in violation of the first criteria. The Defense Data Network is a means of long-haul telecommunications and it would be inappropriate to utilize DDN for intracommand access. An important point here is that DDN is not an office automation technique. Each command connected to the network will be responsible for developing its own internal architecture (this may take the form of multiple processors in a local area network or simply a series of terminals connected to a single host). The purpose of the internal network is two fold. It must contain some form of routing or dissemination process to ensure that the correct user terminal is addressed. In addition, a data base or consolidated process is required so that interfacing to long haul networks can be accomplished at a single point. This is a familiar pattern that will be repeated throughout all levels of access.

Fortunately, the Coast Guard can rely upon the Standard Terminal for intracommand data communications. The microprocessor's clustering ability is ideally suited to meet nearly every unit's internal architectural needs. The

fact that Standard Terminals can also be tied to larger mainframes offers several networking advantages that will be explored in the next section.

C. INTERCOMMAND ACCESS

The subject of intercommand access brings into focus the critical issue of determining the boundary between DDN and other networks within the Coast Guard. For example, should commands separated by a kilometer or so use the Defense Data Network to exchange data communications? The answer is most probably no. Recent technological advances have made it feasible to greatly extend the geographic range of local area networks to meet this type of application. The effect has been to greatly reduce the need to implement more expensive long-haul networking techniques of greater complexity [Ref. 16: pp. 1497-1498]. However, consider the same question if the units are further apart. Then there are two available options; either DDN could be employed or the Coast Guard could rely upon their own long haul networks. Geographic location can also be used to resolve this question.

The Coast Guard approach to networking arose independently from DDN development. Some of the service's efforts, such as ODIN have already been described. One methodology that has not yet been mentioned was to create what is termed regional networks within each District.

Figure 14 shows the district boundaries as well as the location of each District Commander. A regional network can employ a polling scheme compatible with ODIN over Coast Guard leased telecommunication lines. Another alternative is to use the Standard Terminal's X.25 capabilities. Traditionally, regional networks were devoted to teletype applications for record communications but the concept has been expanded to include data communications as well (much of the data communications aspects are still under development). An excellent way to view regional networks is to consider them as non DDN long-haul schemes within a District. The main advantage to this approach is that network boundaries are determined on the basis of operational requirements. A large portion of the service's data communications needs can be handled within s single District, thereby greatly lessening inter-District network congestion. Each District Commander is responsible for developing and maintaining his regional network. Perhaps the most important decision to be made is where to combine two or more commands into a local area network with single regional network access. This depends upon how closely the commands are located and the potential for sharing a common data base. Therefore, the exact configuration of each regional network varies between Districts.

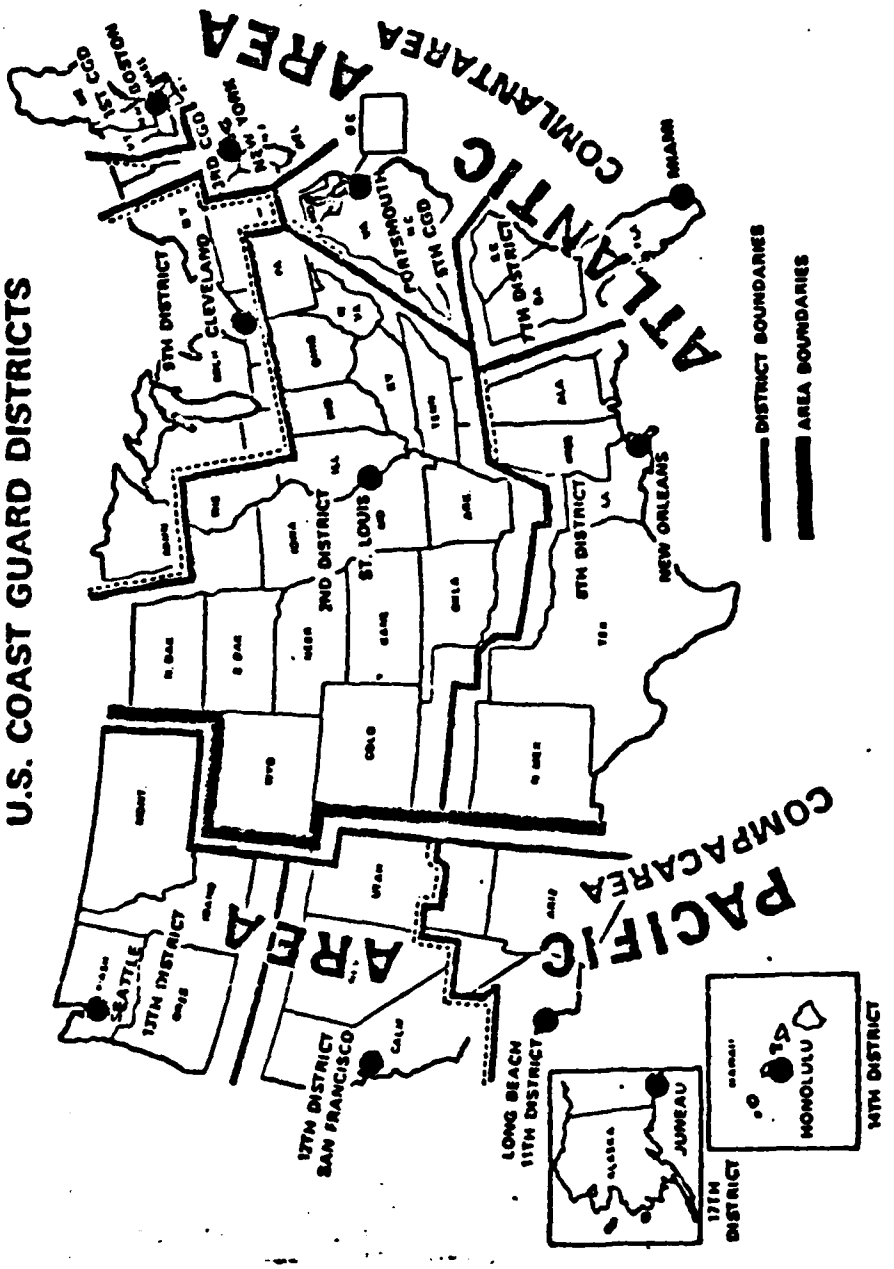


Figure 14. Coast Guard Districts

The focal point for long-haul data communications becomes the headquarters of the District Commander (District Office). District offices now become prime candidates for DDN access. Data exchanges between a District Office host and the Defense Data Network could be handled through a DDN/LAN connection. Other units within a District could access DDN via a regional network. An argument may be made for abolishing the regional networks and directly connecting all LANs to the Defense Data Network. This would indeed eliminate much of the burden on the District offices but the gain is outweighed by the following factors:

1. Each District Office has a computer host mainframe. Smaller units within a District tend to be microprocessor based. As a general rule, it would not be effective to pursue the cost and effort of implementing DDN hardware and software at smaller units.

2. The District offices are the major users of Coast Guard wide computer systems (OPINS, PMIS, etc.).

3. The Coast Guard has experience with regional networks.

4. Regional networks have proven effective for handling record communications and should also perform well for data communications.

5. The communications capability of the Standard Terminal ease local area and regional network development.

There are cases, however, where it is beneficial to provide additional DDN access within a District. This occurs when a District includes a computer resource unit. These commands with large mainframes and data bases serve the entire Coast Guard and should also be connected to the

Defense Data Network. Another logical choice for intercommand DDN access is units which are a part of the Autodin system. This includes Coast Guard Communications Stations and Coast Guard Headquarters, Washington, D.C. Table V shows a complete listing of commands within the service that are recommended to become a part of the Defense Data Network.

This access plan would ensure that all of the computer systems outlined in Section III would effectively be able to utilize DDN. There are several aspects to this plan which should be considered in further detail. First there is a definite possibility that multiple hosts at the same location could share DDN resources. This is especially true in places like Governors Island, New York, where two hosts serving different applications are in the same building. The plan also calls for a complete merger of data and record communications.. For example, each District Office will be required to tie in their computer mainframes with DDN hardware and software to form a comprehensive information processing scheme. This is, of course, the overall intent of both DDN and Coast Guard networking architectures. The success of the effort is crucial to intercommand access issue. It means that an effective hierarchical networking structure could be established between Coast Guard local area, regional and long-haul networks and DDN. This implies not only the elimination of the need for commercial carriers

Table V. Coast Guard Commands that are Recommended for Access to the Defense Data Network

DISTRICT OFFICES	COMPUTER RESOURCE UNITS
CCGDONE Boston, MA.	Operations Computer Center Governors Island, N.Y.
CCGDTWO St. Louis, MO.	Military Pay Center Topeka, KA.
CCGDTHREE Governors Island, N.Y.	MSIS Mainframe (location to be determined)
CCGDFIVE Norfolk, VA.	
CCGDSEVEN Miami, FL.	Autodin Replacement Cites and
CCGD EIGHT New Orleans, LA.	other Commands with Computer Hosts
CCGDNINE Cleveland, OH.	COMMSTA Boston, MA.
CCGDELEVEN Long Beach, CA.	COMMSTA Portsmouth, VA.
CCGDTWELVE San Francisco, CA.	COMMSTA San Francisco, CA.
CCGDTHIRTEEN Seattle, WA.	COMMSTA Honolulu, HA.
CCGDFourteen Honolulu, HA.	RADSTA Guam
CCGDSEVENTEEN Juneau, AK.	COMSTA KODIAK, AK
	AIRSTA Elizabeth City, N.C.
	Group Baltimore, MD.
	CGHQ Washington, D.C.

such as *TELENET* but also total *connectivity*. Any user can invoke whatever data processing application required using this approach.

D. INTERSERVICE ACCESS

The bulk of Coast Guard interservice DDN access will be in the form of traditional record communications message traffic. This is because the Coast Guard is under the Department of Transportation during peacetime and operates under a different set of procedures from the U.S. Navy and the rest of DOD. Therefore, there is little opportunity to utilize most Naval computer applications packages. The two

services do, however, carry out joint operational missions and the need for communications compatibility is ever present. The same rationale that allowed the Coast Guard to become part of the Autodin system also applies to DDN. Since the recommended DDN access plan includes all present Autodin sites, interservice communications should not be adversely affected. The possibility also exists that in special cases, the Coast Guard could utilize Naval data processing resources via DDN. A wartime scenario would call for the full integration of the Coast Guard into the Navy and the Defense Data Network would prove an invaluable tool for this purpose.

E. PERFORMANCE REQUIREMENTS

Table VI presents a summary of DDN projected performance (single-homed subscribers are connected to one node, dual-homed subscribers are connected to two nodes). [Ref. 17: p. 6]. These results are much better than those of Coast Guard long-haul networks especially with regard to delay times and error control. The most important performance characteristics desired by the Coast Guard are in the areas of technical expertise and maintainability. In order to interface Coast Guard mainframes to DDN, the service will require assistance with the more technical aspects of networking. Another consideration is that Coastguardsmen will need training in facilities maintenance

and DDN packet switching concepts to minimize downtime. Clearly, once a DDN access plan is finalized the Coast Guard and the U.S. Navy will be required to develop an interservice agreement on these issues as well as provisions for hardware and software. The Coast Guard must be able to establish their networking requirements as well as understand the potential of DDN to be integrated into the services data communications architecture. This is one of the primary objectives of this thesis.

Table VI. Projected Performance of the Defense Data Network

AVAILABILITY	
For Single-homed Subscribers	99.00%
For Dual-homed Subscribers	99.95%
END-TO-END DELAY	
Average:	
For High-Precedence Traffic	0.090 Seconds
For Routine-Precedence Traffic	0.122 Seconds
Ninety-Ninth Percentile	
For High-Precedence Traffic	0.224 Seconds
For Routine-Precedence Traffic	0.458 Seconds
PROBABILITY OF UNDETECTED ERROR	4.2×10^{-18}
PROBABILITY OF MISDELIVERING PACKET	5.5×10^{-12}

V. FUNCTIONAL REQUIREMENTS

A. THE NEED FOR FUNCTIONAL REQUIREMENTS

The discussion to this point has centered around system applications and network architectures for determining the best use of the Defense Data Network by the U.S. Coast Guard. In simpler terms, emphasis has been placed on answering the who,what, and why questions of this issue. Now the time has come to explore how DDN can be connected to local area and regional networks. The focus shifts from computer networks and their components (architecture) to the exact hardware and software specifications (implementation) required to achieve networking goals [Ref 18: p. 215]. The preferred method of accomplishing this is through the use of functional modules. A functional module description contains the precise purpose of a particular hardware device or program. The advantage to a functional approach is that many applications can utilize a common set of functional modules to avoid redundancy. It no longer becomes necessary to define a separate data communications scheme for each system application for example. Thus precious networking resources are used in the most effective manner [Ref: 19, p. 2]. This does not imply that architectural or applications matters are unimportant in functional design. These form the basis for a networking effort. The functional approach

is a mechanism for achieving desired results and therefore must always be consistant with application and architectural goals.

The end result of a functional design is one or more implementation block diagrams. This allows for the tracing of a data communications path from source to destination through each applicable functional module. Several familiar patterns will emerge when describing this flow. First it is necessary to point out the input requirements to each module. Then, the process within a module will be discussed and finally the outputs are determined. Functional modules are in effect individual building blocks. Each relies heavily on others for specific purposes. One of the main problems in computer networking is that designers must be able to understand both macro and micro perspectives. Great care must be taken to ensure that overall system concepts and individual key elements are distinguished. Otherwise the true purpose of functional modules becomes lost in a maze of complex technicalities.

The functional requirements of Coast Guard/DDN interconnection will be discussed in terms of hardware, software and security. Once again it should be pointed out that these are artificial distinctions for the purpose of simplification. In fact it is impossible to separate the three aspects and still have an effective network. The physical and logical viewpoints of Section II will serve as

starting point for this more advanced networking explanation.

B. HARDWARE

The functional requirements for hardware are relatively simple to understand. There are only three reasons for invoking computer hardware. They are:

1. To process a user application.
2. To gain access to a network.
3. To move data through a network.

The first category of hardware consists primarily of Coast Guard mainframes and microprocessors. Examples include the Operations Computer Center, Standard Terminals and District Office minicomputers. Section III adequately described these resources as well as the primary Coast Guard user applications. The third category is principally the Defense Data Networks backbone structure. This is merely the collection of IMPs that move packets through the subnetwork in the manner explained in Section II. The most important developmental hardware type to make the proposed Coast Guard/DDN architecture a reality becomes devices that grant DDN access. These processors make the continuous data flow through the hierarchical networking structure possible.

Figure 15 shows the various ways that the Defense Data Network may be accessed. [Ref. 17: p. 8] Host mainframes can be directly tied to DDN. This will require that all DDN

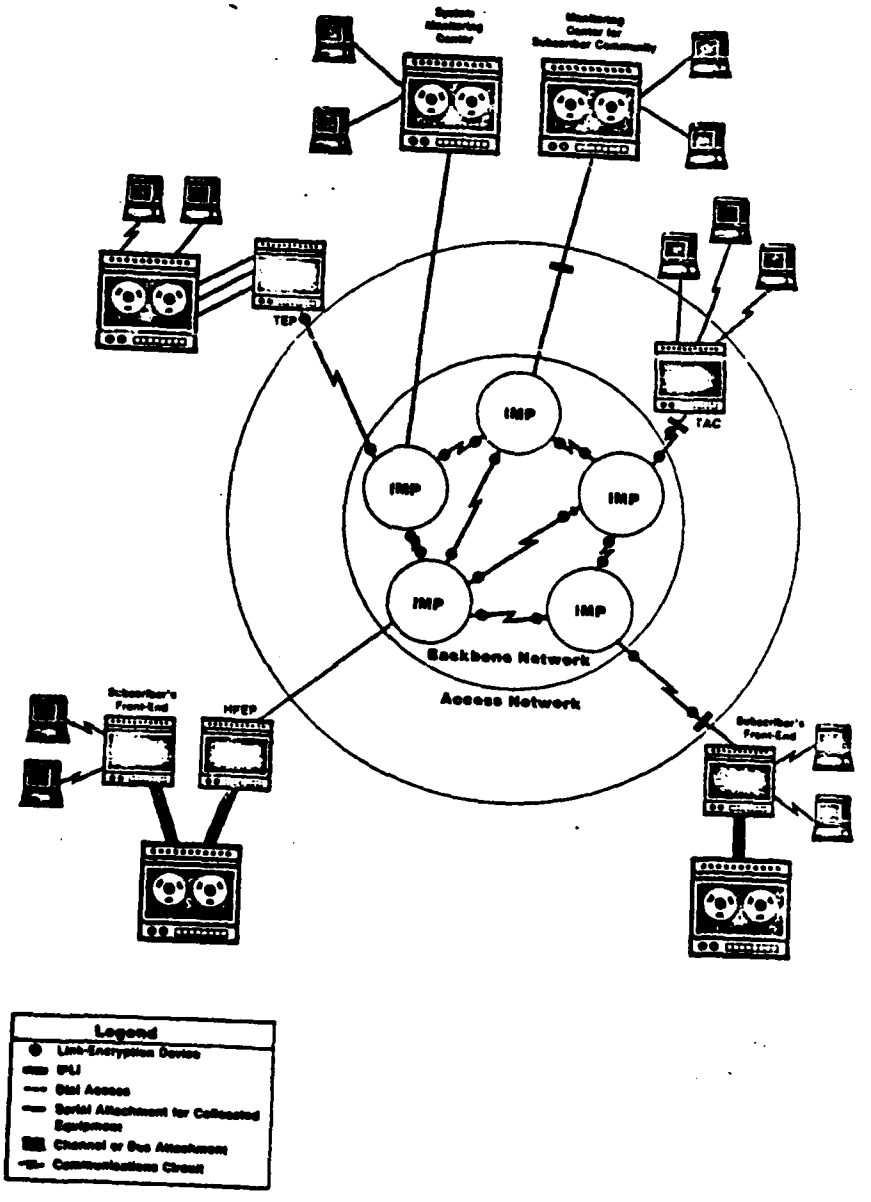


Figure 15. DDN Access Hardware

protocols reside within the subscriber host. The direct host implementation can employ full DDN networking services such as establishing host-to-host terminal-to-host and host-to-terminal connections [Ref. 7: p. 163]. The main disadvantage to this approach is that valuable computer capacity, designed for user applications, is taken up with DDN networking protocols.

Another alternative is to provide host access through the use of a front-end-processor. This device is itself a computer designed specifically for handling host to network data communications thereby eliminating the burden on user applications mainframes. The DDN-developed Host Front-End Processor (HFEP) connects on one side to the subscriber's mainframe bus or I/O channel. The HFEP contains all of the required protocols to allow for full DDN networking services and connections to the backbone. [Ref. 7: p. 164]. In addition,users may develop their own front-end processors for access to DDN or other networks.

There is one other method that a user host may be tied into the Defense Data Network. A device called a Terminal Emulation Processor can link a mainframe's terminal ports to a backbone IMP. Even though the TEP has DDN protocols, the host mainframe appears logically to be only a set of connected terminals. Full networking services are unavailable and therefore this access approach is not recommended [Ref. 7: p. 164].

Individual terminals can be linked to the Defense Data Network in two ways. The most obvious method is via a subscriber host. Another alternative is to utilize a Terminal Access Controller as described in Section II. Connection to a TAC may be established via serial attachment for colocated equipment, a communications circuit, or by telephone dial in. Initially, the Defense Communications Agency was opposed to dial in access because of security reasons. However, dial in access has since been allowed with the stipulation that tight controls be instituted to prevent unauthorized entry into the network. [Ref. 7: p. 19].

The DDN access picture is completed with the addition of network monitoring centers. DDN developed monitoring centers were outlined in Section II. It is also possible for a subscriber community to establish their own monitoring capability.

The most critical hardware issue is determining which access method best suits Coast Guard needs. One important fact to remember is that Figure 15 represents access to only one network, DDN. The primary concern of the Coast Guard as subscribers is to also connect the service's regional and some local area networks to form the entire network architecture. The best choice is to utilize front-end processors for host access. This is because the Coast Guard has made no allowance for implementing DDN protocols in

their mainframes and the TEP does not have full network service capabilities. However, the major design issue is not the access of one host but rather the interconnection of other networks.

The access plan of Section V has taken into account the need to translate from single host to local area and regional networks. The consolidation of DDN data communications at District Office mainframes serves this purpose. It appears from the Defense Data Network perspective that one host (the District Office mainframe) has access through a front-end processor. In reality this host serves as the focal point for data communications for not only the District Commander, but also those connected to the regional network. This implies that each District Office mainframe would be required to have substantial telecommunications capabilities. The most beneficial situation would be to have a single front-end processor for all networking needs at each District. Unfortunately, this is difficult for practical reasons. The HFEP has been designated for use for DDN access only and not other networks. This leaves the Coast Guard with two options, 1) develop a subscriber front-end that can access all Coast Guard networks and DDN. 2) Utilize the HFEP for DDN access and other means for local area and regional networks. The second alternative is probably the most preferred since it saves a great deal of research and development in DDN

protocol implementation. For the most part, Coast Guard networks use communications software that is installed in the same processors that handle user applications. Therefore, most District Offices do not require separate front-end processors for local area and regional networks. This option is available however if additional mainframe capacity is desired.

Figure 16 shows a simplified hardware block diagram assuming that the HFEP is the only required front-end processor. A Standard Terminal local area network within a District accesses the District Office host via a regional network. In turn, the District Office host is connected to an intracommand regional network, a HFEP and the Coast Guard's long haul ODIN network.

These same principles can be applied to computer resource units and other commands that require DDN access and are not a District Office. The Coast Guard could also take advantage of Terminal Access Controllers. A Standard Terminal can be connected to a TAC it is using the asynchronous terminal emulator feature. DDN can then be used to grant access to other hosts (and through Coast Guard hosts, regional and local area networks). The dial-in feature of the TAC and the simplicity of the connection make this alternative attractive in cases where a user application host is not required at a particular location.

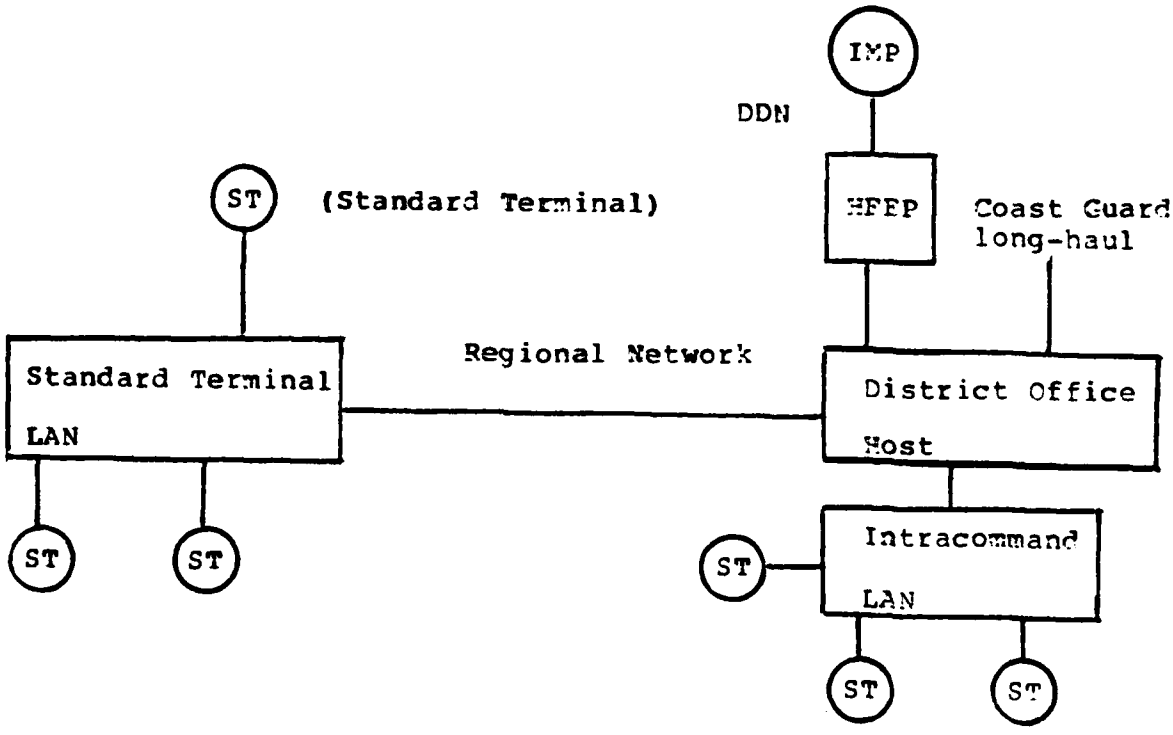


Figure 16. A Typical Example of a Coast Guard Multiple Network Connection.

C. SOFTWARE

1. The Importance of Protocols

The fact that the Coast Guard and DDN hardware require interconnection to form a network architecture is readily apparent. However, no hardware explanation alone could possibly describe the functional implementation process. The key to the successful integration of Coast

Guard local area and long-haul networks with DDN primarily rests with the ability to determine required protocols. Section II provided the basic description of a protocol. Recall that protocols serve to grant access, handle packets through the backbone, and establish a means of end-to-end control by means of a layering process.

The common protocol between Coast Guard and DDN networks is X.25. It may appear that the best way to handle packets in the physical data link and network layers would be to invoke X.25 at all locations where Coast Guard and DDN access is desired. Unfortunately, this methodology will not produce the desired interconnection in the near future. The Defense Communications Agency has emphasized that the only supported DDN access means is via a Protocol called 1822 along with TCP and IP. [Ref 15: p. 3]. There are two major problems with a X.25 implementation for DDN. The first is that there are a large variety of incompatible X.25 packages available which could cause serious operational problems for DDN users [Ref 15: p. 3]. Secondly, the X.25 virtual circuit approach is in direct conflict with the DDN philosophy of utilizing datagrams for communications within the backbone or network layer. It will most probably take a substantial period of time to resolve these difficulties. Therefore, it is recommended that the Coast Guard adopt the existing 1822/IP/TCP implementation for DDN networking. It is entirely possible that the Coast Guard may desire to

change to a X.25 implementation when a good X.25 DDN standard is agreed upon. However, it should be noted that this would eliminate the need for the 1822 protocol only. TCP and IP would still be required for DDN communications. Below is a listing of all of the needed protocols for the Defense Data Network along with a brief description of their purpose [Ref. 17: p. 13]:

Transmission Control Protocol/Internet Protocol (TCP/IP)--permits end-to-end flow of data between two computer systems or between a host and a TAC.

File Transfer Protocol (FTP)--a protocol that allows for the transfer of files between hosts.

Telnet--A virtual terminal protocol that converts different terminal types to common virtual terminal format for use throughout the network. (This is not to be confused with TELENET the commercial dial in service).

Volumes of information is available on these protocols. The descriptions provided herein are merely brief summaries of the functional aspects of DDN software. An attempt will be made to define these protocols in terms of the layer of operation, specification of services, and the interaction of a particular protocol with protocols of other layers [Ref. 20: p. 625]. The reader is referred to the Defense Data Network Program Plan for a more detailed explanation of DDN protocols. An excellent discussion of IP and TCP can also be found in the October, 1980 issue of the

ACM Computer Communications Review.

2. The 1822 Protocol

The 1822 Protocol roughly corresponds to the physical and data link layers of the ISO model. Its primary use is for establishing the host to IMP or TAC to IMP access connection for the Defense Data Network. The protocol was initially developed by the Bolt Beranek and Newman Corporation for the ARPANET and found acceptable for use with DDN. [Ref. 7: p. 154] One of the main services provided by the protocol (besides host-to-IMP connection) is that it allows for location independent addressing. This means that connections may be referred to physically and logically thereby permitting multiple users without additional hardware interfacing. The 1822 local host option has a distance limitation of 2000 feet. This distance can be increased through the use of modems and the 1822 Distant Host or Very Distant Host option [Ref. 7: pp. 154-155]. The protocol will normally reside within the HFEP in cases where front-end devices are used for DDN access. When the X.25 protocol is available for DDN use, access can also be gained through High-Level Data Link Control (HDLC). HDLC is a protocol found within X.25 at the data link layer.

3. The Internet Protocol

Once access to the DDN backbone is obtained, the internet protocol (along with IMP to IMP protocol) is

responsible for packet switching through the subnetwork. There are two basic requirements for this service: the physical address of source and destination. The purpose of IP is to move datagrams independently through the backbone. This means that each packet must contain an internet header. In keeping with the true nature of datagrams, there are no provisions for data reliability, flow control or sequencing. Therefore, end-to-end acknowledgement is impossible with IP and reliable communications are not guaranteed [Ref. 18: pp. 15-16]. Packets are routed through the subnetwork via the routing algorithm described in Section II. Since the control of packets is not maintained with IP, packets are given a finite lifetime in the network to avoid congestion problems.

The internet protocol derives its name form the fact that it also serves outside of the DDN backbone for interconnecting networks. There are three basic parameters required to perform this function; 1) The name of the resource being sought (what), 2) The address of the resource (where), 3) The route to be taken (how), [Ref. 22: p. 614]. The last two items are handled via the internet protocol and IMP-to-IMP communications schemes. The name of a resource is actually a symbol or logical address of a particular process, device, or service [Ref. 22: p. 614]. This parameter comes from the higher level TCP protocol. One problem that can occur is that packet sizes between networks

may differ. In this case it is necessary to split packets and later reassemble them for transmission through other networks. Therefore, IP has provisions for packet fragmentation for this purpose [Ref. 21: p. 20]. In summary, the internet protocol allows multiple networks to share a convention for packet addressing, routing and fragmentation. This concept in computer networking is called a gateway [Ref. 4: pp. 638-639].

Appendix B contains a description of the IP header. A diagram of the header format and a description of header fields is provided. (Some fields were not described in the text but their explanations in pointed out in the appendix. [Ref. 21: pp. 22-25].

4. The Transmission Control Protocol

The Transmission Control Protocol is designed to provide reliable host-to-host communications between packet switched networks, particularly DDN. [Ref. 23: p. 54] In other words, TCP must be able to overcome the inadequacies of the internet protocol with regard to end-to-end control. TCP and IP are in fact extremely dependent on each other in the protocol layering implementation process [Ref. 24: p. 55]. The transmission control protocol is on of the most versatile (and therefore one of the most complex) protocols in the field of computer networking. Here is a listing of

TCP services along with a brief description of the protocols implementation approach:

a) Basic Data Transfer--TCP allows users to send or receive a continuous stream of data and prepares packets for transmission via the internet protocol [Ref. 24: p. 57].

b) Reliability--TCP provides for end-to-end acknowledgement of packets and the retransmission of unreceived packets [Ref. 23: p. 57]. This means that the protocol establishes packet sequencing for error detection and the correct reassembling of packets [Ref. 4: p. 643].

c) Flow Control--TCP allows the receiver to govern the amount of data transmitted through the use of windows [Ref. 4: p. 643]. This concept was described in Section II.

d) Multiplexing--a single host is allowed multiple processors through the use of TCP. This means that the protocol establishes the logical naming of different processors. [Ref. 23: p. 58].

e) Connections--TCP provides for a logical host-to-host connection. The user has the ability to monitor the status of host connections. [Ref. 23: p. 58].

f) Precedence and Security--The user may indicate the precedence and security of computer communications.

Details of the TCP header are contained in Appendix C. The transmission control protocol plays a key role. It is the users interface with the network allowing control of the host-to-host communications process. At the same time it interacts with the internet protocol to ensure reliable end-to-end transfer of data. Item e, is a particularly interesting feature. In order to communicate between hosts the user must establish a logical connection through TCP. Actual commands such as OPEN, CLOSE and STATUS deal

specifically with this logical connection [Ref. 23: pp. 62-63]. Notice that the overall effect has been to transform the backbone datagram process into a host-to-host virtual circuit process [Ref. 8: pp. 32-33]. These are some of the most revolutionary concepts in computer networking. The speed of independent travelling datagrams is combined with the reliability of virtual circuit service in one network! This result is the reason for the warning of maintaining perspective in computer networking. The function of protocols must be tied to the layers in which they serve. Also the distinction between physical and logical connection and addressing is of paramount importance. Hopefully this difference will be more clearly pointed out in Section V-C-6.

5. The File Transfer and Telnet Protocols

These two protocols deal primarily with specific user applications and are therefore lumped together in this subsection even though they perform separate functions. Both FTP and Telnet rely upon the networking capabilities established by the 1822/TCP/IP protocols.

The file transfer protocol accomplishes exactly what the name implies. It allows a user to transfer files from one host to another. This basically means that a set of conventions have been agreed upon for file structure. Examples include controls for start of file, end of text, end of file, etc. Users will be required to possess file

formats that make use of this protocol [Ref. 17: p. 13]. Normally this is not a problem. FTP has demonstrated its flexibility to accommodate a variety of file structures.

Telnet allows a user to appear that his terminal is directly connected to a foreign host. The protocol creates a common set of terminal characteristics known as a network virtual terminal (NVT) [Ref. 7: p. 158]. This becomes a standard format for all terminals in the entire network and embraces the TCP/IP inter-networking capabilities [Ref. 17: p. 13].

6. The Internetworking of Coast Guard/DDN Software

The protocols discussed up to this point will allow a host to utilize the full services of DDN. However, the access plan of Section III requires the addition of Coast Guard local area and regional networks. The DDN method of interconnecting networks (gateways) has already been described. The problem of continuing this approach into Coase Guard networks is that DDN software would be required at each user processing point. A more economical procedure would be to connect multiple local area networks to a single host for long-haul networking [Ref. 16: p. 1498]. This is precisely the idea behind Coast Guard regional networks. In effect each District Office host also serves as a gateway. This is not a TCP/IP Defense Data Network gateway but rather a local area/regional to DDN transfer. The difference is

that 1822/TCP/IP need not be contained in processors below the District Command level.

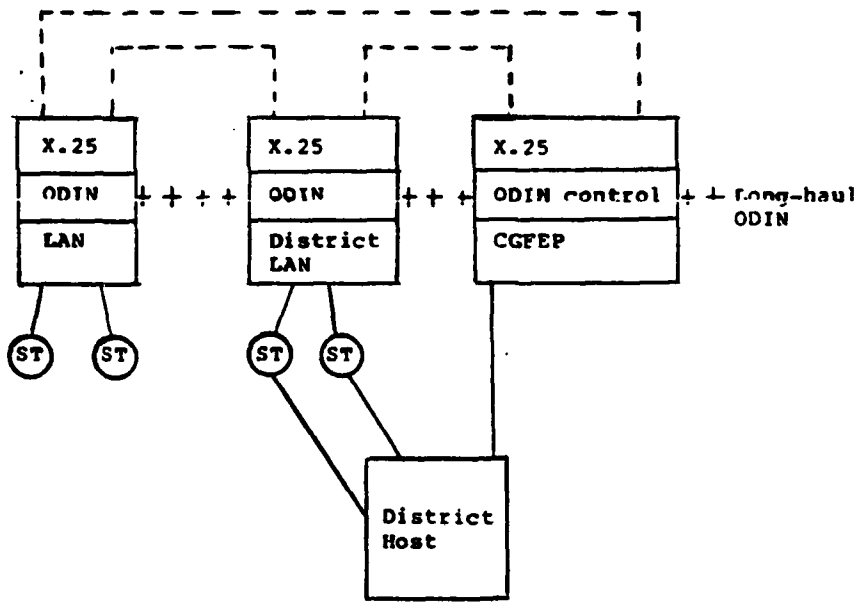
This alternative seems quite attractive but unfortunately the functional requirements for such an arrangement are often difficult to determine and theoretical in nature. In the past, local area technology has lagged behind long-haul network development but this gap is constantly being shortened [Ref. 16: pp. 1497-1498].

The U.S. Coast Guard has one major advantage over most other subscribers who may attempt connecting multiple local area networks to DDN at one gateway. Standard Terminal configurations can bridge long-haul and local area networks. Internal software to the device makes it possible to cluster microprocessors to form local area networks as well as provide remote data communications via an X.25 polling scheme. The key developmental area is the establishment of the District Office multiple gateway. The Standard Terminal regional network must be tied to the minicomputer mainframe. For the sake of clarity, it will be assumed that each District host will have two front-end processors. One will handle DDN communications (HFEP) and the other will serve the regional network. This second device will be designated as a Coast Guard front-end processor (CGFEP). The distinction is made for illustrative purposes. In actuality, the case may be that all

communications software resides in a single front-end or some/all protocols are internal to Coast Guard mainframes.

Figure 17 shows the software block diagram for the regional network connection (notice that the addition of the CGFEP also calls for a hardware modification). The regional network is established via X.25 and polling protocols (ODIN). Terminals at the District Office LAN may be linked to the regional network and/or directly to a mainframe port. This allows terminals at the District to be a part of the regional network and also process user applications directly from the co-located host. The CGFEP can control the ODIN polling process or establish virtual circuits between the host and local area networks. In either case its primary responsibility rests with physical and logical addressing and data routing. It may not be necessary to include both X.25 and ODIN in all instances. However, one possibility is that polling could be used for interservice long-haul network traffic while X.25 is designated exclusively for regional communications. This would allow local area networks to form virtual circuits independent of the host. Figure 17 represents only two local area networks (the District LAN plus one other). In reality, the District regional network will be comprised of more LANS. The figure was kept simple for ease of understanding.

The last stage of the interconnection problem is to tie together the two host front-end processors to complete



Legend

—— Direct connection

+++ Polled circuit

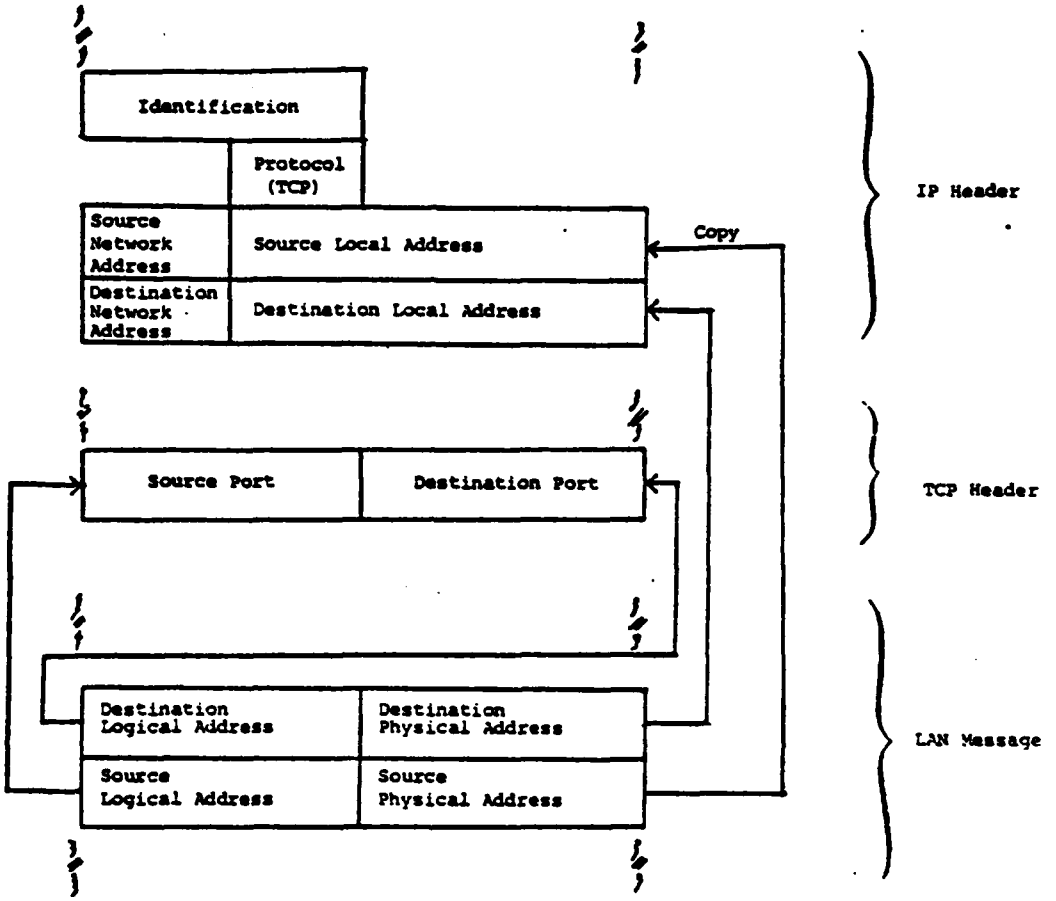
(ST) Standard Terminal

- - - Virtual circuit

Figure 17. A Coast Guard Regional Network

the overall network architecture. One of the pioneers in developing the functional requirements for the interfacing of local area networks to DDN is Professor Norman Schneidewind of the U.S. Naval Postgraduate School. Many of the concepts described below can be found in his report entitled, Functional Design of a Local Area Network for the Stock Point Integrated Communications Environment, December, 1982. [Ref. 25]

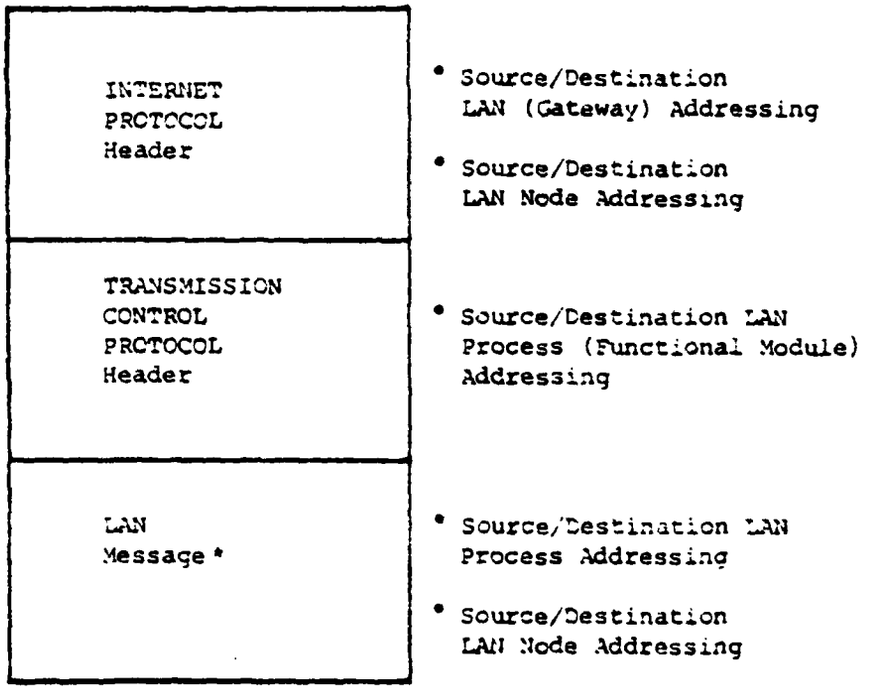
The crux of the problem rests with converting the regional network message formats to suitable DDN packets. This is accomplished with the insertion of a National Communications functional module (NC) [Ref. 25: p. 27]. This module performs two major services. The first to be described is protocol convention. The LAN message is transformed into one compatible with DDN. This requires that the physical and logical addresses of the process are transferred from the local area message to the headers in TCP and IP. Figure 18 illustrates this important idea [Ref. 25: p. 37]. The TCP header receives the logical address for virtual circuit services. The IP header obtains the physical address of source and destination. This allows for the NC to perform its section function of the creation of datagram packets [Ref. 25: p. 28]. Figure 19 shows the entire internet datagram [Ref. 25: p. 36]. This simple figure points out a profound networking concept. The addresses (both physical and logical) of the LAN header are



IP
- Identification: Identifier used By IP to Reassemble All Fragments Belonging to a Datagram (Value Provided by TCP)
- Protocol: Identifies Next Protocol Above IP (i.e., TCP)
- Source Network Address: Address of Source LAN
- Source Local Address: Address of Source LAN Physical Node
- Destination Network Address: Address of Destination LAN
- Destination Local Address: Address of Destination LAN Physical Node

TCP
- Source Port: Source Logical Address
- Destination Port: Destination Logical Address

Figure 18. Internet Datagram Showing Fields of IP Header, TCP Header and LAN Message Which are Relevant to Addressing



* Complete message or fragment

Figure 19. An Internet Datagram

embedded in the internet packet [Ref. 4: p. 639]. The appropriate address is summoned when the pertinent protocol is activated. This is known as header wrapping [Ref. 25: p. 33]. Thus it is possible to trace data communications through both Coast Guard networks and DDN by studying the protocol header address at a given time. The Coast Guard multiple gateway will be required to handle all of the physical and logical addresses for source and destination for the entire internetworking scheme. The identity of the correct host, local area network, and process in a virtual sense must be maintained along with its physical location.

Figure 20 shows the Coast Guard/DDN functional requirement block diagram for hardware and software [Ref. 25: p. 35]. By adding the NC to the Coast Guard front-end processor, the interconnection between the regional network and DDN is established. This example assumes data communications between a Coast Guard host/local area networks and DDN is desired. It is also possible to form a communications path between regional networks by creating a mirror image of a regional network on each side of the HFEP devices. Each portion of this figure has been discussed within this section so there is no need to repeat an explanation of these functional requirements. There are, however, several aspects to the network structure that are not shown in Figure 20. One is that regional communications will most probably not be conducted at the same speed as the

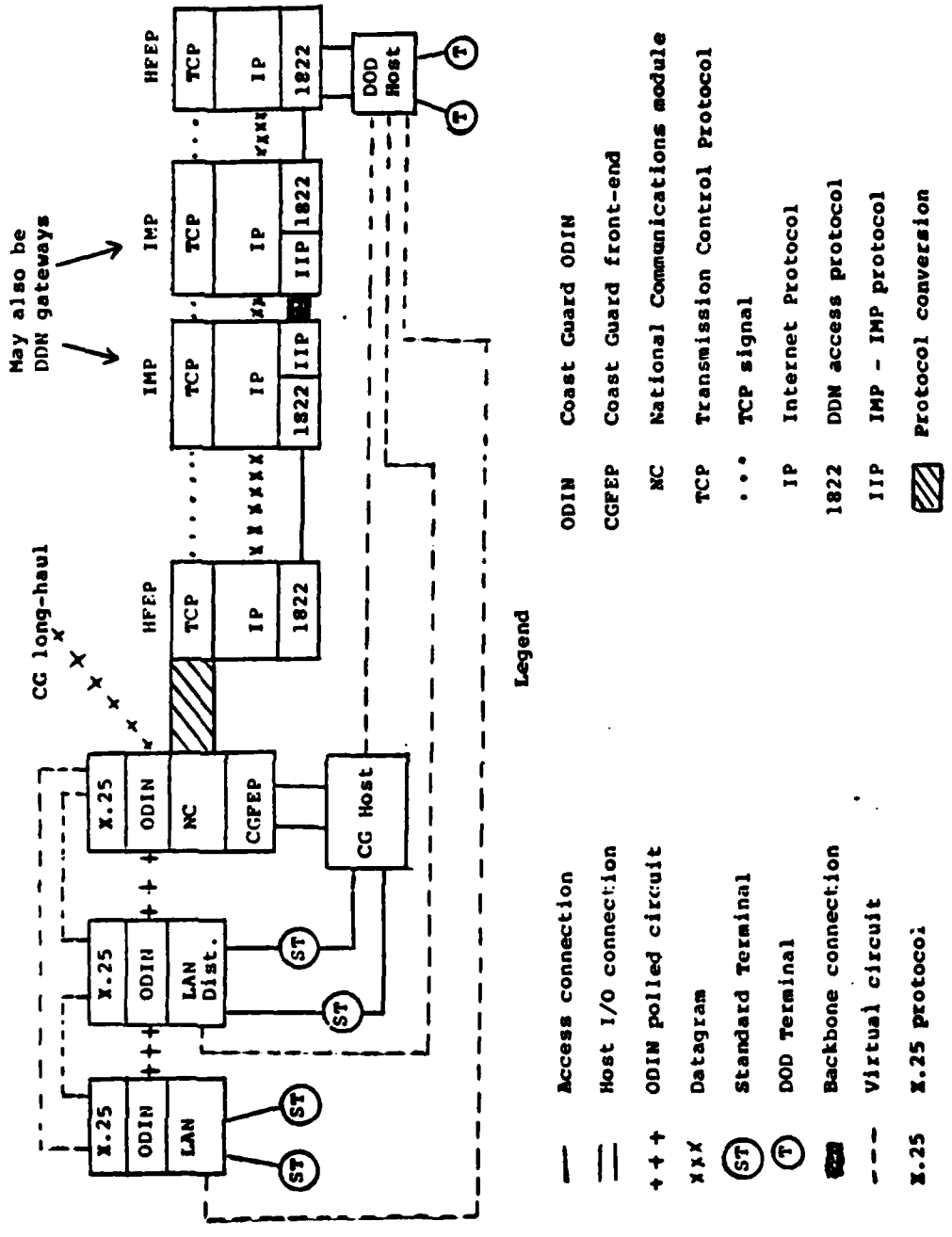


Figure 20. The Coast Guard/DDN Internetworking Connection

Defense Data Network. Therefore, it will be necessary to buffer data to prevent overflows [Ref. 25: p. 28]. The buffers will exist between the Coast Guard host, regional network and the HFEP. Figure 20 also does not how protocols that are above the transport layer. It is assumed that for Coast Guard inter-command applications, the Standard Terminal will have the required additional software. In cases where Coast Guard /DOD communications are applicable, TELNET, FTP or some other agreed upon set of higher level protocols will be needed. Finally recall that there are DDN access provisions other than through front-end processors. In particular, the Coast Guard may desire to take advantage of the Standard Terminal to TAC DDN connection in some instances.

D. SECURITY AND IMPLEMENTATION TIMETABLE

Section II introduced the IPLI device and the separation of user communities cryptographically for security purposes. Figure 21 shows all of the safeguards of DDN to support security and privacy [Ref. 17: p. 10]. These measures include [Ref. 17: p. 11];

1. Link encryption on all backbone links and classified host and TAC access links.
2. End to end encryption by IPLI devices.
3. A cryptographic authentication code will be used by Monitoring Centers to prevent unauthorized transmission of packet switching control messages.

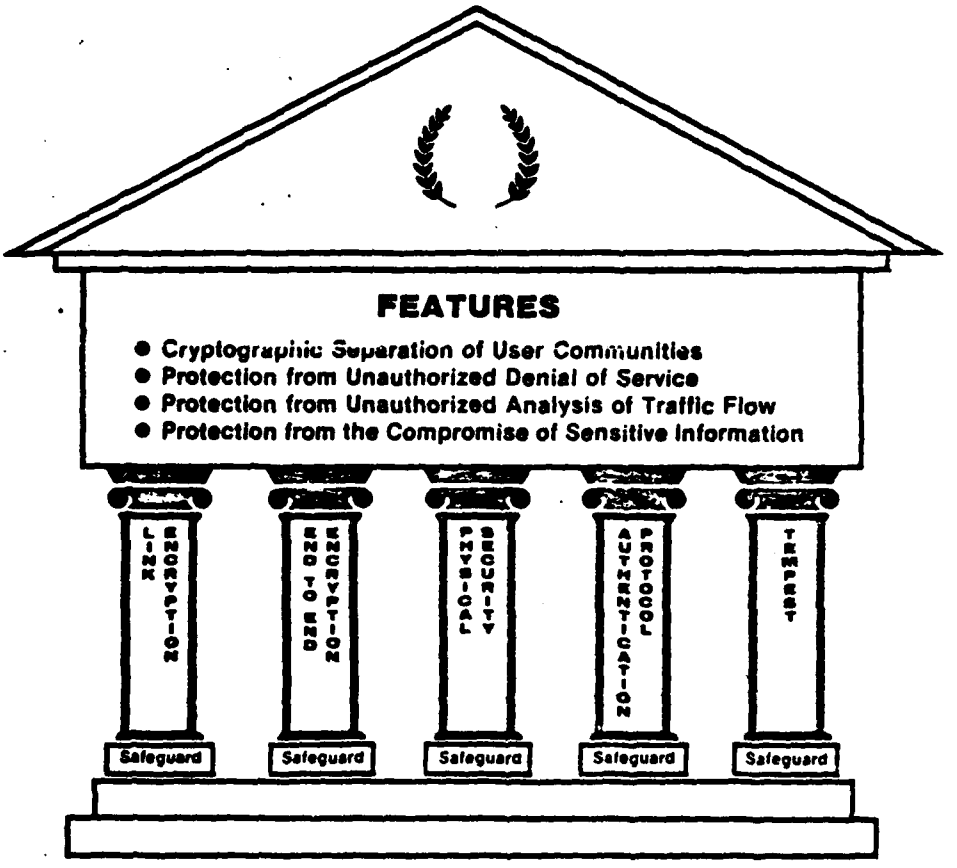


Figure 21. The Safeguards to Support Security and Privacy Features

4. Physical security measures will be taken to protect classified data.

5. Network elements will be TEMPEST-approved.

Most probably the Coast Guard should become a partitioned user community from the rest of the subscribers of DDN. One potential networking problem is that the Coast Guard's planned secure C3 system will be incompatible with DDN. The designers of the C3 system should be cautioned against this possibility if the service desires Coast Guard/DDN secure data communications. This thesis does not deal with secure inter-networking because the Coast Guard has not yet finalized a scheme for the C3 system.

The IPLI units will not become fully available until approximately the middle of 1985. In the meantime, military unclassified users of the ARPANET will branch out to form a DDN segment called MILNET. This phase of implementations has already begun and includes over half of the previous ARPANET subscribers. The ARPANET will continue to exist as a research and development tool. Once all of the IPLI devices become available the entire Defense Data Network will be completed [Ref. 17: pp. 21-22]. The Coast Guard, U.S. Navy and the Defense Communications Agency have yet to formalize a DDN implementation schedule for the Coast Guard. Hopefully, their agreement will be completed during the late 1983 early 1984 timeframe and will contain many of the recommendations of this thesis.

VI. CONCLUSIONS

Computer networks have reached the stage of development where it is not longer necessary to tailor data communications to a specific user application. Both the Department of Defense and the U.S. Coast Guard have recognized that it is now possible to share computer resources in an economical fashion to meet all information processing needs. This is particularly evident in the desire to communicate traditional military message traffic and other computer data by using the same network architecture. The DOD approach to overcoming hardware and software incompatibility problems is to implement the packet switched Defense Data Network. On the other hand, the coast Guard has chosen to institute network hierarchies and install processors that can be implemented under a variety of data communications schemes. Each method has its advantages and set-backs. The Defense Data Network can interconnect multiple long-haul networks but requires additional development to form the local area/DDN interface. The Coast Guard has bridged the local area/long-haul network gap by the use of Standard Terminals but compatibility problems still occur when data transits form one long-haul network to another.

This thesis has described both approaches and recommended an integrated Coast Guard/DDN network architecture. Since most Coastguardsmen are unfamiliar with DDN, an attempt was made to fully develop the implications of packet switching and Defense Data Network methodology. The implementation of the recommended architecture was based upon hardware and protocol functional requirements. The success of this effort will depend on the Coast Guard's ability to develop a front-end processor that can fulfill the data communications requirements of local area networks, host mainframes and DDN. The critical element is to create a mechanism to transfer physical and logical addresses as data travels through the network hierarchy. The Coast Guard has begun this development with networks internal to the service. *It is most strongly recommended that the scope of* the effort be extended to include a means of interacting with the national communications module to provide full DDN services.

It may appear to some that it is not worth the trouble and expense to interconnect computer networks. The truth of the matter is that the Armed Forces, or any other user of multiple computers, can ill afford to operate and maintain incompatible systems. Communications problems have plagued man since the Tower of Babel. Each successful attempt to overcome these difficulties has resulted in rewards that far overshadow the cost.

APPENDIX A

DEFENSE DATA NETWORK HARDWARE COST

COSTING MODEL

In general, costs have the following components: a direct hardware capital cost, a monthly maintenance cost, and installation cost and a one-time integration cost. The monthly maintenance cost is computed as 1.75% of the direct hardware cost. The installation cost is a one-time cost which is computed as 5.25% of the direct hardware cost. The integration cost is charged only for non-BBN products. This is computed as 15% of the direct hardware cost. These rates apply to all hardware items in the design with the exception of KG-84 encryption devices.

MULTIPLEXERS (TEMPEST, HEMP)

The cost of connecting a terminal to a TAC is the cost of the multiplexer (if used), the cost of the line, the cost of KG's (if needed) and the cost of the TAC port. In the cost model, multiplexers are priced on a per channel basis, where there is one channel for each terminal whose data is multiplexed. The per channel costs have been computed assuming that there is a multiplexer at both ends of the line and that the multiplexers meet both Tempest and HEMP requirements. The costs per channel for a multiplexer are:

hardware cost:	$2124.00
maintenance cost:	$ 37.17
installation cost:	$ 111.51
integration cost:	$ 318.60

TAC (TEMPEST, HEMP)

TACs handle up to 16 terminals. There is a base cost associated with a TAC in addition to a cost for each TAC port that is used by a terminal. The TACs are assumed to meet Tempest and HEMP requirements.

base hardware cost:	$7500.00
additional hardware cost per port:	$ 250.00
base maintenance cost (per month):	$ 131.25
added maintenance cost per port (per month):	$ 4.38

base installation cost:	$ 393.75
added installation cost per port:	$ 13.13

KG-84

The KG-84 costs are computed in a different manner from other elements. In particular, it is assumed that monthly maintenance costs equal .5% of the hardware cost and that the installation cost is 1.5% of the hardware cost. There is no additional integration cost for the KG.

base hardware cost:	$5000.00
maintenance cost (per month)	$ 25.00
installation cost:	$ 75.00

IPLI (TEMPEST, HEMP)

The IPLI includes a KG-84. The prices below are for the IPLI alone, exclusive of the KG.

base hardware cost:	$15000.00
maintenance cost (per month):	$ 262.50
installation cost:	$ 787.50

The cost of an IPLI with a KG is therefore:

base hardware cost:	$20000.00
maintenance cost (per month):	$ 287.50
installation cost:	$ 862.50

MODEMS (HEMP)

The unit costs for modems are as follows:

Speed	Cost	Maintenance (per month)	Installation	Integration
300	$1835.00	$32.11	$96.34	$275.25
1200	$1965.00	$34.39	$103.16	$294.75
2400	$2885.00	$50.49	$151.46	$432.75
4800	$4416.00	$77.28	$231.84	$662.40
9600	$6221.00	$108.87	$326.60	$933.15

C/30 IMP (TEMPEST, HEMP)

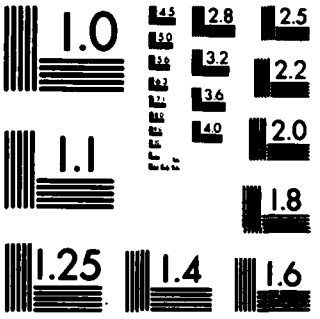
There is a base cost for a C/30 plus a cost for each port used by hosts TACs or trunks.

base hardware cost:	$44636.00
added hardware cost per port:	$ 152.00
base maintenance cost (per month):	$ 781.13

AD-A136 783 A PLAN FOR THE ACCESS AND UTILIZATION OF THE DEFENSE DATA NETWORK BY THE UNITED STATES COAST GUARD(U) NAVAL POSTGRADUATE SCHOOL MONTEREY CA E A LANE SEP 83 2/2

UNCLASSIFIED F/G 17/2 NL

END
DATE FILMED
2-84
DTIC



MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

added maintenance cost per port (per month):	$ 2.66
base installation cost:	$ 2343.39
added installation cost per port:	$ 7.98

LINE COSTS

All lines less than or equal to 9600 bps are priced according to the ATT 3002 tariff. Wideband lines (19.2 and 56 Kbps) are priced according to the DDS tariff with 19.2 Kbps lines priced exactly as 56 Kbps lines. Installation costs are not considered in computing line costs.

There are two components to the tariffs used by the design algorithms: a fixed monthly charge and a mileage dependent charge. The tariffs as provided by DCA are as follows:

Speed = 110, 150, 300, 1200, 2400, 4000, 4800, 9600
Fixed Component = $105.34

miles	1-15	2.55 per mile
miles	16-25	2.13 per mile
miles	26-100	1.59 per mile
miles	101-1000	.93 per mile
miles	1000-	.57 per mile

Speed = 19200, 56000
Fixed Component = $1271.20

miles	1-15	$12.75 per mile
miles	16-25	$10.65 per mile
miles	26-100	$ 7.95 per mile
miles	101-1000	$ 4.65 per mile
miles	1000-	$ 2.85 per mile

EXPANSION FACTORS FOR OVERSEAS TARIFFS

To compute the cost of a line for which at least one terminus is not within CONUS, the costs given in the previous section are multiplied by an expansion factor for the first 1000 miles. Line cost for the portion of the line greater than 1000 miles, are calculated using CONUS tariffs. The expansion factors were provided to the design teams. The expansion factor used depends upon the line's endpoints. For this purpose, the world is divided into three areas, defined as follows:

CONUS:	65	< longitude	< 164
Pacific	164	< longitude	< 180
	-180	< longitude	< -60
Europe	-60	< longitude	< 65

The expansion factors for lines are:

CONUS<->CONUS:	1.0
CONUS<->Europe:	3.3
CONUS<->Pacific:	4.9
Europe<->Europe:	2.5

APPENDIX B

INTERNET PROTOCOL FUNCTIONAL SPECIFICATION

A summary of the contents of the internet header follows:

Version	IHL	Type of Service	Total Length
Identification		Flags	Fragment Offset
Time to Live	Protocol		Header Checksum
Source Address			
Destination Address			
Options			Padding

Figure 22. Example Internet Datagram Header

Version: 4 bits

The Version field indicates the format of the internet header. This document describes version 4.

IHL: 4 bits

Internet Header Length is the length of the internet header in 32 bit words, and thus points to the beginning of the data.

Type of Service: 8 bits

The Type of Service provides an indication of the abstract parameters of the quality of service desired. These parameters are to be used to guide the selection of the actual service parameters when transmitting a datagram through a particular network. Several networks offer service precedence, which somehow treats high precedence traffic as more important than other traffic. A few networks offer s Stream service, whereby one can achieve a smoother service at some cost. Typically this involves the reservation of resources within the network. Another choice involves a low-delay vs. high-reliability trade off. Typically networks invoke more complex (and delay producing)

mechanisms as the need for reliability increases. The type of service is used to specify the treatment of the datagram during its transmission through the internet system as follows:

```
Bits  0-2:   Precedence.
Bit     3:   Stream or Datagram.
Bits  4-5:   Reliability.
Bit     6:   Speed over Reliability.
Bit     7:   Speed.
```

Total Length: 16 bits

Total Length is the length of the datagram, measured in octets, including internet header and data.

Identification: 16 bits

An identifying value assigned by the sender to aid in assembling fragments of a datagram.

Flags: 3 bits

Various Control Flags.

```
Bit 0: reserved, must be zero
Bit 1: Don't Fragment This Datagram (DF).
Bit 2: More Fragments Flag (MF).
```

Fragment Offset: 13 bits

This field indicates where in the datagram this fragment belongs. The fragment offset is measured in units of 8 octets (64 bits). First fragment has offset zero.

Time to Live: 8 bits

This field indicates the maximum time the datagram is allowed to remain in the internet system. If this field contains the value zero then the datagram should be destroyed. This field is modified in internet header processing. The time is measured in units of seconds. The intention is to cause undeliverable datagrams to be discarded.

Protocol: 8 bits

This field indicates the next level protocol used in the data portion of the internet datagram.

Header Checksum: 16 bits

A checksum on the header only. Since some header fields may change (e.g., time to live), this is recomputed and verified at each point that the internet header is processed.

Source Address: 32 bits

The source address. The first octet is the Source Network, and the following three octets are the Source Local Address.

Destination Address: 32 bits

The destination address. The first octet is the Destination Network, and the following three octets are the Destination Local Address.

Options: variable

The option field is variable in length. There may be zero or no options. There are two cases for the format of an option:

Case 1: A single octet of option-type.

Case 2: An option-type octet, an option-length octet, and the actual option-data octets.

The option classes are:

0 = control
1 = internet error
2 = experimental debugging and measurement
3 = reserved for future use

APPENDIX C

TRANSMISSION CONTROL PROTOCOL FUNCTIONAL SPECIFICATION

TCP segments are sent as internet datagrams. The Internet Protocol header carries several information fields, including the source and destination host addresses. A TCP header follows the internet header, supplying information specific to the TCP protocol. This division allows for the existence of host level protocols other than TCP.

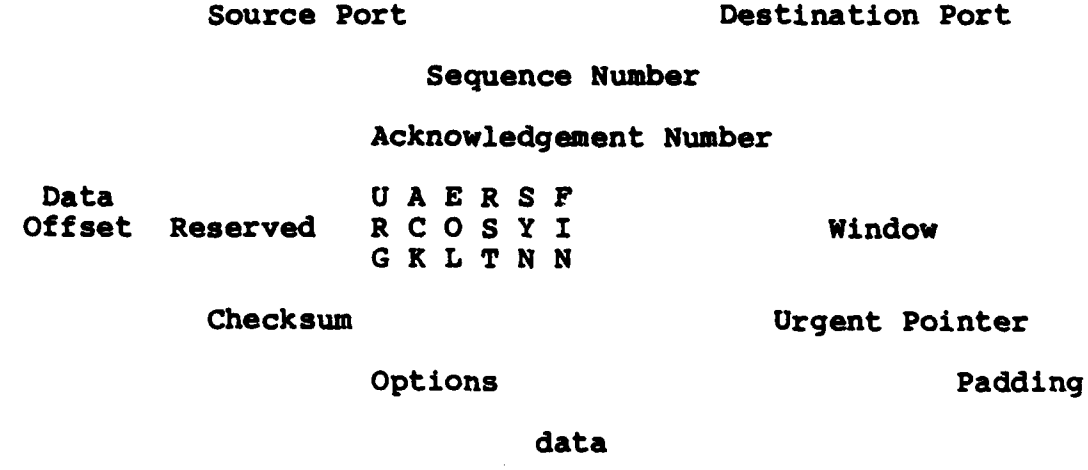


Figure 23. TCP Header Format

Source Port: 16 bits

The source port number.

Destination Port: 16 bits

The destination port number.

Sequence Number: 32 bits

The sequence number of the first data octet in this segment (except when SYN is present).

Acknowledgment Number: 32 bits

If the ACK control bit is set this field contains the value of the next sequence number the sender of the segment is expecting to receive. Once a connection is established this is always sent.

Data Offset: 4 bits

The number of 32 bit words in the TCP Header. This indicates where the data begins. The TCP header including options is an integral number of 32 bits long.

Reserved: 6 bits

Reserved for future use. Must be zero.

Control Bits: 8 bits (from left to right):

URG: Urgent Pointer field significant
ACK: Acknowledgment field significant
EOL: End of Letter
RST: Reset the connection
SYN: Synchronize sequence numbers
FIN: No more data from sender

Window: 16 bits

The number of data octets beginning with the one indicated in the acknowledgment field which the sender of this segment is willing to accept.

Checksum: 16 bits

The checksum field is the 16 bit one's complement of the one's complement sum of all 16 bit words in the header and text. If a segment contains an odd number of header and text octets to be checksummed, the last octet is padded on the right with zeros to form a 16 bit work for checksum purposes.

The checksum also covers a 96 bit pseudo header conceptually prefixed to the TCP header. This pseudo header contains the Source Address, the Destination Address, the Protocol, and TCP length. This gives the TCP protection against misrouted segments. This information is carried in the Internet Protocol and is transferred across the TCP/Network interface in the arguments or results of calls by the TCP on the IP.

Urgent Pointer: 16 bits

This field communicates the current value of the urgent pointer as positive offset from the sequence number in this segment. The urgent pointer points to the sequence number of the octet following the urgent data. This field should only be interpreted in segment with the URG control bit set.

Options: variable

Options may occupy space at the end of the TCP header and are a multiple of 8 bits in length. All options are included in the checksum. An option may begin on any octet boundary. There are two cases for the format of an option:

Case 1: A single octet of option-kind.

Case 2: An octet of option-kind, an octet of option-length, and the actual option-data octets.

Currently defined options include (kind indicated in octal):

Kind	Length	Meaning
0	-	End of option list.
1	-	No-Operation.
100	-	Reserved.
105	4	Buffer Size.

Padding: variable

The TCP header padding is used to ensure that the TCP header ends and data begins on a 32 bit boundary. The padding is composed of zeros.

LIST OF REFERENCES

1. Kuo, F.F., Protocols and Techniques for Data Communications Networks, pp. 2-4, 125, Prentice-Hall, 1981.

2. Commander, Naval Telecommunications Command Letter Serial 02/2299 to Defense Data Network Subscribers, Subject: Defense Data Network (DDN) Requirements Identification, 29 July 1982.

3. Kleinrock, L., "Principles and Lessons in Packet Communications", Proceedings of the IEE, v. 66, no. 11, pp. 1320-1329, November, 1978.

4. Cerf, V.G., and Kahn, R.E., "A Protocol for Packet Network Intercommunication", IEEE Transactions on Communications, v. com-28, no. 4, pp. 637-647, April, 1980.

5. Tanenbaum, A.S., Computer Networks, pp. 8,16,150,188,189,369-370, Prentice-Hall, 1981.

6. Cerf, V.G., and Kirstein, P.T., "Issues in Packet-Network Interconnection", Proceedings of the IEE, v. 66, no. 11, pp. 1386-1407, November, 1978.

7. Defense Communications Agency, Defense Data Network Program Plan, pp. 2-5,19,67,106,154-155,158,163,164,179, January, 1982.

8. McQuillan, J.M., Richer, I., and Rosen, E.C., "The New Routing Algorithm for the ARPANET", IEEE Transactions on Communications, v.com-28, no.5, pp. 711-715, May 1980.

9. Greene, W. and Pooch, V.W., "A Review of Classifications Schemes for Computer Communications Networks", Computer, pp. 12-19, November, 1977.

10. Corrigan, M.Z., "Defense Data Network Protocols", Conference Record, EASCOM 82, IEEE, pp. 131-135, September, 1982.

11. Rybcznski, A., "X.25 Interface and End-to-End virtual Circuit Service Characteristics", IEEE Transactions on Communications, v.com-28, no. 4, pp. 500-512, April 1980.

12. Cerf, V.G., and Lyons, R.E., "Military Requirements for Packet-Switched Networks and Their Implications for Protocol Standardization", Conference Record, EASCOM 82, IEEE, pp. 119-129, September, 1982.

13. Selvaggi, P.S., "The Department of Defense Protocol Standardization Program," Conference Record, EASCOM 82, IEEE, pp. 111-118, September, 1982.

14. United States Coast Guard, Command, Control and Communications (C3) Plan, COMDINST M3090.1, pp. 1-9,1-10, 6 May 1983.

15. Nicholson, C.M., Coast Guard Information Architecture Concept Paper, an Internal Coast Guard Paper, pp. 5-1,9-5,9-6,11-14, 11 February 1982.

16. Clark, D.D., Pogran, K.T., and Reed, D.P., "An Introduction to Local Area Networks", Proceedings of the IEEE, v. 66, no. 11, pp. 1497-1516, November, 1978.

17. Defense Communications Agency, Defense Data Network, a Subscriber Informatio Brochure, pp. 6,8,10,11,13,21,22, March, 1983.

18. Green, P.E., "An Introduction to Network Architectures and Protocols", IBM Systems Journal, v. 18, no. 2, pp. 202-221, January 1979.

19. Schneidewind, N.F., Functional Approach to the Design of a Local Area Network: A Naval Logistics System Example, Paper Presented at the IEEE Computer Society Spring Computer Conference 83, Washington, D.C., March, 1983.

20. Bochmann, G.V., and Sunshine, C.A., "Formal Methods in Communication Protocol Design", IEEE Transactions on Communications, v. com-28, no. 4, pp. 624-630, April 1980.

21. Postel, J.B., ed., "DOD Standard Internet Protocol", ACM Computer Communications Review, v. 10, no. 4, pp. 14-51, October, 1980.

22. Boggs, D.R., and others, "Pup: An Internetwork Architecture", IEEE Transactions on Communications, v. com-28, no. 4, pp. 612-623, April 1980.

23. Deputy Secretary of Defense Memorandum to Secretaries of the Military Departments, Subject: Defense Data Network (DDN) Implementation, 10 March 1983.

24. Postel, J.B., ed., "DOD Standard Transmission Control Protocol", ACM Computer Communications Review, v. 10, no. 4, pp. 52-132, October, 1980.

25. Naval Postgraduate School Report NPS-54-82-003, Functional Design of a Local Area Network for the Stock Point Logistics Integrated Communications Environment, by N.F. Schneidewind, pp. 28, 33, 35, 37, December, 1982.

INITIAL DISTRIBUTION LIST

		No. Copies
1.	Defense Technical Information Center Cameron Station Alexandria, Virginia 22314	2
2.	Library, Code 0142 Naval Postgraduate School Monterey, California 94943	2
3.	Department Chairman, Code 54 Department of Administrative Sciences Naval Postgraduate School Monterey, California 93943	1
4.	Professor Norman F. Schneidewind Code 54 Ss Naval Postgraduate School Monterey, California 93943	1
5.	CDR Gary R. Porter, Code 55 Pt Department of Operations Research Naval Postgraduate School Monterey, California 93943	1
6.	Commandant (G-PTE) United States Coast Guard Washington, D.C. 20593	2
7.	Commandant (G-TPP) United States Coast Guard Washington, D.C. 20953	2
8.	LT Edward A. Lane 2435 Windbreak Drive Alexandria, Virginia 22306	4